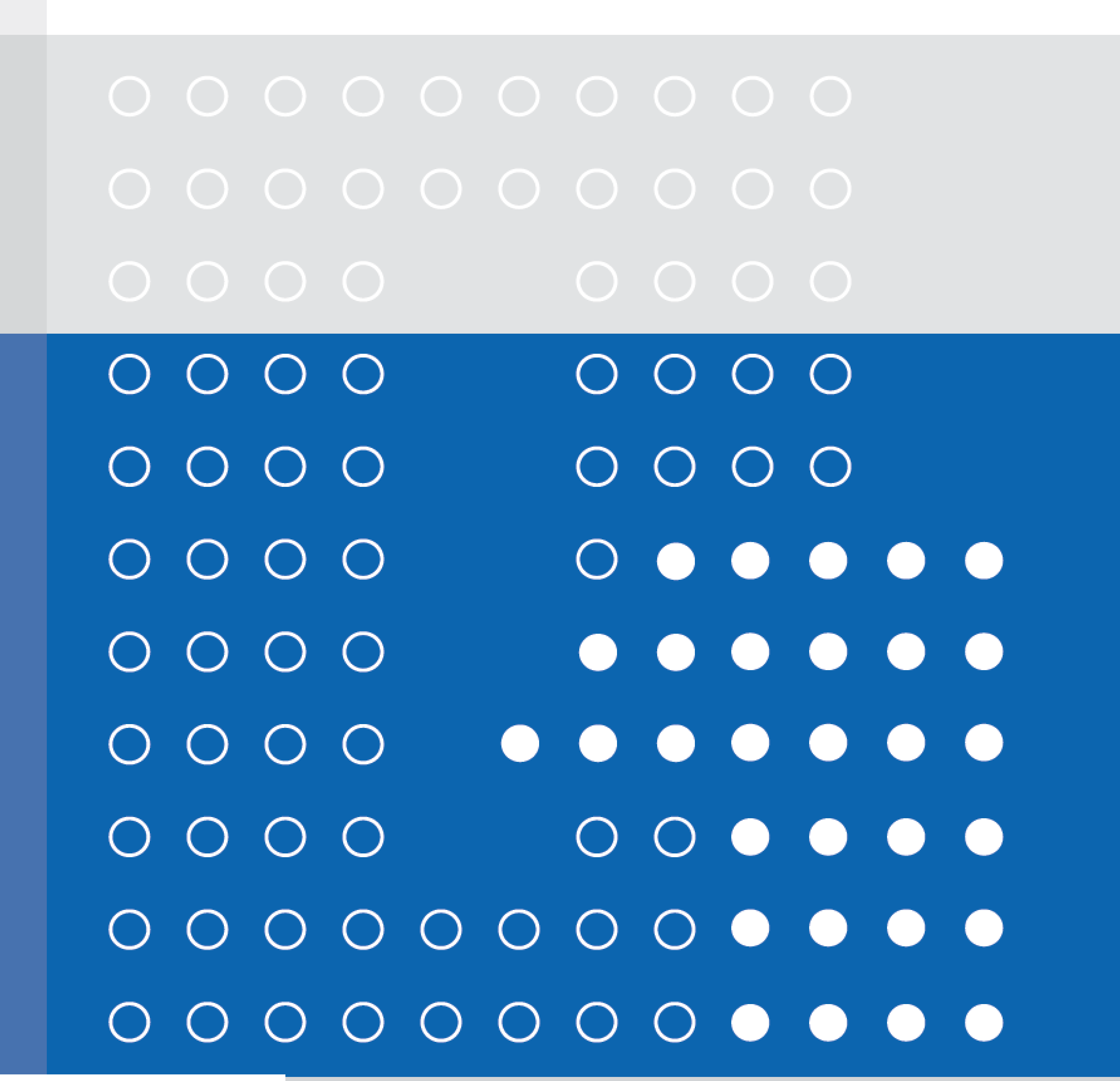
计算机系列教材

网络安全综合实践教程



蒲晓川 成爱民 阮清强 唐晔 林朝晖 编著

清华大学出版社

计算机系列教材

网络安全综合实践教程

蒲晓川　成爱民　阮清强　唐　晔　林朝晖　编著

清华大学出版社
北　　京

内 容 简 介

实践教学是巩固基本理论和基础知识、提高学生分析问题和解决问题能力的有效途径，是应用型本科院校培养具有创新意识的高素质应用型人才的重要环节。

本实验课程属于专业教育课程，授课对象为掌握一定网络安全技术原理、密码技术和计算机网络技术等的学生。本实验课程的开设对于锻炼学生的网络安全综合保障技能，提高分析解决实际问题的能力，在掌握基本技能的基础上提高应用创新等方面的能力有重要影响。

网络安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别 7 个方面。本书按照该原则组织实验项目。

本实验课程中所有的实验项目都在实验室展开，不在互联网中进行，遵守国家法律，不会危及互联网的安全。

图书在版编目(CIP)数据

网络安全综合实践教程/蒲晓川等编著. --北京：清华大学出版社，2016
计算机系列教材
ISBN 978-7-302-42495-6

Ⅰ. ①网…　Ⅱ. ①蒲…　Ⅲ. ①计算机网络－安全技术－教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 316463 号

责任编辑：白立军　王冰飞
封面设计：常雪影
责任校对：李建庄
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：三河市君旺印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：10.75　　**字　　数**：265 千字
版　　次：2016 年 3 月第 1 版　　**印　　次**：2016 年 3 月第1 次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：066982-01

前 言

本实验课程属于专业教育课程，授课对象为掌握一定网络安全技术原理、密码技术和计算机网络技术等的学生。本实验课程的开设对于锻炼学生的信息安全综合保障技能，提高分析解决实际问题的能力，在掌握基本技能的基础上提高应用创新等方面的能力，有重要影响。

在完成该实验课程的学习后，应能够达到了解信息安全的体系结构和基本内容，了解信息安全的实体安全和运行安全，掌握和运用基本的信息安全技术，能够综合分析信息安全事件，解决信息安全问题，做好信息安全保障等要求。

信息安全的研究范畴目前还没有一个统一的定义。按照“计算机信息系统安全专用产品分类原则(GA 163—1997)”，信息安全产品分为实体安全、运行安全和信息安全 3 个方面。其中，实体安全包括环境安全、设备安全和媒体安全 3 个方面；运行安全包括风险分析、审计跟踪、备份与恢复、应急 4 个方面；信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别 7 个方面。本书就是按照这个原则组织实验项目的。

本实验课程的前期课程包括计算机网络、网络安全技术、反病毒技术、网络攻防对抗实验、军事理论与信息对抗等。

本书由蒲晓川确定研究内容和整体结构，其中，3.1 节、3.9 节由成爱民编写，其他章节由蒲晓川编写。

由于时间紧、任务重，本书难免存在一些问题，望广大师生给予批评指正。

作　者

2016 年 2 月

EDITORS

目 录

第 1 章　概　　述

1.1　课程简介

21 世纪是一个以网络为核心的信息时代。世界经济正在从工业经济向知识经济转变，知识经济的两个重要特征就是信息化和全球化。信息化已经成为当今世界经济和社会发展的趋势，这种趋势主要表现在：①信息技术突飞猛进，成为新技术革命的领头羊；②信息产业高速发展，成为经济发展的强大推动力；③信息网络迅速崛起，成为社会和经济活动的重要依托。信息比例的加大使得社会对信息的真实程度、保密程度的要求不断提高，而网络化又使因虚假、泄密引起的信息危害程度呈指数增大。针对信息的有意刺探、攻击行为更是国家、单位重点防护的事件。

全球信息安全的形势严峻。针对信息的保护与反保护等行为一直伴随着信息的整个发展历程。进入 21 世纪后，信息安全面临着更严峻的考验。国内外的网络信息安全事件主要表现在系统的安全漏洞不断增加、黑客攻击搅得全球不安、计算机病毒肆虐、网站仿冒、木马和后门程序泄露秘密、信息战阴影威胁数字化和平和白领犯罪造成巨大商业损失等。

在完成本实验课程的学习后，能够达到了解信息安全的体系结构和基本内容，了解信息安全的实体安全和运行安全，掌握和运用基本的信息安全技术，能够综合分析信息安全事件，解决信息安全问题，做好信息安全保障等要求。

本实验课程中的所有实验项目都在实验室展开，不会危及互联网的安全。

目前，还没有现成的网络安全对抗实验教材供我们参考，编者经过认真研究和调查分析，结合我校学生的具体情况，特制定该课程的实验体系，如表 1-1-1 所示。信息安全的研究范畴目前还没有一个统一的定义。按照“计算机信息系统安全专用产品分类原则(GA 163—1997)”，信息安全产品分为实体安全、运行安全和信息安全 3 个方面。其中，实体安全包括环境安全、设备安全和媒体安全 3 个方面；运行安全包括风险分析、审计跟踪、备份与恢复、应急 4 个方面；信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别 7 个方面。本“信息安全综合实验”课程就是按照这个原则组织实验项目的。

表 1-1-1　《信息安全综合实验》实验体系

序号	实 验 题 目	实验类型	实验学时	选择要求
1	剩磁效应与数据恢复	验证型	2	必选
2	操作系统安全评估与检测	综合型	4	必选
3	数据加密与鉴别	综合型	8	必选
4	数据库安全	综合型	4	课外自选
5	网络安全通信	综合型	4	必选

续表

序号	实验题目	实验类型	实验学时	选择要求
6	数字证书服务及加密认证	综合型	8	必选
7	访问控制和网络防火墙	综合型	8	必选
8	入侵检测	综合型	4	必选
9	Internet 服务器安全	综合型	4	必选
10	网络安全程序设计	设计型	8	课外自选
11	应用程序保护	设计型	4	课外自选
12	网络监控与协议分析	综合型	4	必选
13	风险分析	设计型	2	课外自选
14	安全审计与追踪	综合型	4	课外自选
15	应急响应与灾难恢复	设计型	4	课外自选

1.2 实验类型

实验的分类方法很多，按性质可分为验证型实验、设计型实验和综合型实验 3 种类型。

1. 验证型实验

验证型实验作为一种重要的实验形式，无论在科学研究中还是科学教育中，都是不可或缺的，其作用也是任何其他类型的实验所无法替代的。验证型实验主要培养学生对设备、开发工具的操作能力，加深对理论的理解。实际上，与课程相关的大部分实验都是验证型实验。实验设计者给出较为详细的实验步骤，旨在减少实验者摸索的过程，争取在较短的时间内掌握基本的操作技术。

验证型实验的方法：

（1）明确实验题目、实验目的和实验要求；

（2）熟悉实验背景知识；

（3）按照实验内容进行实验；

（4）分析实验结果，完成实验报告。

2. 设计型实验

设计型实验培养学生的设计能力和独立工作的能力。这类实验是课程中较大的实验。也就是在基本训练的基础上，提出一些有利于启发思维、有应用价值的实验课题，让学生进行设计型实验。题目描述以提出任务、要求和阐述应用背景为宜，而如何解决问题，解决问题的原理、方法和所用仪器等由同学们自行提出并实践，目的是使学生运用所学的理论知识和实验技能，在实验方法的考虑、使用工具的选择、测试方法的确定等方面受到比较系统的训练。

设计型实验的方法：

(1) 了解题目要求，明确任务；

(2) 查阅有关资料，画出必要的原理图，寻求各种解决问题的方法。从原理、方法和使用工具等多方面提出完成课题任务的依据及实验步骤；

(3) 设计并实现设计内容；

(4) 测试结果评价，总结分析并完成实验报告。

3. 综合型实验

综合型实验是指实验内容涉及本课程的综合知识或与本课程相关课程的知识的实验，其主要教学目的是培养学生综合运用知识分析、解决实际问题的能力以及创新能力。

综合型实验的方法：

(1) 了解题目要求，明确实验任务；

(2) 根据已经掌握内容，查阅有关资料，综合利用各种方法、工具策略等完成实验；

(3) 分析实验结果，总结并完成实验报告。

第2章　实验要求

2.1　实验过程要求

在实验过程中，实验者必须服从指导教师和实验室工作人员的安排，遵守纪律与实验制度，爱护设备及卫生。在指定的实验时间内，必须到机房内实验，其余时间可自行设计和分析。

由于实验时间有限，要求提前预习实验内容，对于一些基本概念不再进行详细解释说明，实验课程授课的理论部分重点放在实验方法分析方面。

(1) 验证型实验：实验前，预习实验，了解实验背景。按照实验指导书的方法步骤进行实验，将实验结果与理论分析结果进行比较，得出结论，按要求写出实验报告。注意掌握基本的实验方法。

(2) 设计型实验：严格要求自己，自信但不固执，独立完成设计任务，善于接受指导教师的指导和听取同学的意见，有意识地树立严谨的科学作风，要独立思考，刻苦钻研，勇于创新，按时完成设计任务。

(3) 综合型实验：要充分发挥主动性和创造性，要求综合运用所掌握的知识，完成实验任务。按照指导书要求的实验任务，完成实验方案论证与设计、实验过程和实验报告。

2.2　考核及评分标准

本课程采用结构化评分，其中，验证型实验占40%，综合型、设计型实验45%，其他15%(主要由指导教师根据考勤、课程表现等把握)。验证型实验、设计型实验和综合型实验主要考核指标如下。

(1) 验证型实验：实验者是否真实、认真地完成了本次实验；实验代码是否规范、可读性怎样、效率怎样；实验报告格式是否规范，是否有抄袭行为等。

(2) 设计型实验：设计代码是否调试通过、运行结果是否正确，是否具备良好可读性；设计报告是否层次清楚、整洁规范、有无相互抄袭情况。答辩分为自述和教师提问两部分，自述时间不得超过5分钟，内容包括演示、描述本课题设计思想、关键代码分析等。

(3) 综合型实验：实验者对所学知识的综合运用情况、综合分析情况；实验报告是否层次清楚、整洁规范、有无相互抄袭情况。答辩分为自述和教师提问两部分，自述时间不得超过5分钟，内容包括对于本实验目的的理解、实施方案、实验结果情况及分析等。

第3章 实验内容

3.1 数据恢复

3.1.1 实验类型

验证型，2 学时，必选实验。

3.1.2 实验目的

计算机磁盘属于磁介质，所有磁介质都存在剩磁效应的问题，保存在磁介质中的信息会使磁介质不同程度地永久性磁化，所以磁介质上记载的信息在一定程度上是抹除不净的，通过一定的技术手段可以将已抹除信息的磁盘上的原有信息提取出来。

另外，由于计算机文件系统的实现原理，文件的删除并没有将文件的数据内容从磁盘上删除，通过一定的技术手段可以将删除的文件恢复出来。

通过该实验，使学生认识到电磁泄露现象引起的数据恢复、硬件损坏、文件删除等实现数据恢复的内容。

3.1.3 题目描述

使用数据恢复软件 EasyRecovery 进行文件恢复。

3.1.4 实验要求

理解磁盘数据恢复的原理，认识数据恢复技术对信息安全的影响。能够使用数据恢复软件 EasyRecovery 进行文件恢复。

提高要求：能够对磁盘数据进行彻底清除。

3.1.5 相关知识

1. 剩磁效应

计算机主机及其附属电子设备，如视频显示终端、打印机等，在工作时不可避免地会产生电磁波辐射，这些辐射中携带有计算机正在进行处理的数据信息。尤其是显示器，由于显示的信息是给人阅读的，是不加任何保密措施的，所以其产生的辐射是最容易造成泄

密的。使用专门的接收设备将这些电磁辐射接收下来，经过处理，就可恢复还原出原信息。

国外对计算机设备的辐射问题早已有研究，在1967年的计算机年会上美国科学家韦尔博士发表了阐述计算机系统脆弱性的论文，总结了计算机4个方面的脆弱性，即处理器的辐射、通信线路的辐射、转换设备的辐射和输出设备的辐射。这是最早发表的研究计算机辐射安全的论文，但当时没有引起人们的注意。1983年，瑞典的一位科学家发表了一本名叫《泄密的计算机》的小册子，其中再次提到计算机的辐射泄露问题。1985年，荷兰学者艾克在第三届计算机通信安全防护大会上公开发表了他的有关计算机视频显示单元电磁辐射的研究报告，同时在现场做了用一台黑白电视机接收计算机辐射泄露信号的演示。他的报告在国际上引起强烈反响，从此人们开始认真对待这个问题。据有关报道，国外已研制出能在一千米之外接收还原计算机电磁辐射信息的设备，这种信息泄露的途径使敌对者能及时、准确、广泛、连续而且隐蔽地获取情报。计算机电磁辐射泄密问题已经引起了各个国家的高度重视，要防止机密信息被窃取，必须采取防护和抑制电磁辐射泄密的专门技术措施，这方面的技术措施有干扰技术、屏蔽技术和Tempest技术。

计算机磁盘属于磁介质，所有磁介质都存在剩磁效应的问题，保存在磁介质中的信息会使磁介质不同程度地永久性磁化，所以磁介质上记载的信息在一定程度上是抹除不净的，使用高灵敏度的磁头和放大器可以将已抹除信息的磁盘上的原有信息提取出来。据一些资料的介绍，即使磁盘已改写了12次，但第一次写入的信息仍有可能复原出来。这使涉密和重要磁介质的管理以及废弃磁介质的处理都成为很重要的问题。国外有的甚至规定记录绝密信息资料的磁盘只准用一次，用后必须销毁，不准抹后重录。

2. 文件删除原理

存储在硬盘中的每个文件都可分为两部分：文件头和存储数据的数据区。文件头用来记录文件名、文件属性、占用簇号等信息。文件头保存在一个簇并映射在FAT表（文件分配表）中，而真实的数据则是保存在数据区当中的。平常所做的删除，其实是修改文件头的前两个代码，这种修改映射在FAT表中，就为文件做了删除标记，并将文件所占簇号在FAT表中的登记项清零，表示释放空间，这也就是平常删除文件后，硬盘空间增大的原因。而真正的文件内容仍保存在数据区中，并未得以删除。要等到以后的数据写入，把此数据区覆盖掉，才算是彻底把原来的数据删除。如果不被后来保存的数据覆盖，它就不会从磁盘上抹掉。用Fdisk分区和Format格式化和文件的删除类似，只是前者改变的是分区表，后者修改的是FAT表，都没有将数据从数据区直接删除。

3. 某一分区被误格式化或文件丢失或误删除的恢复

对于FAT格式的文件结构，文件删除仅仅是把文件的首字节改为E5H，其余的内容并没有被修改，因此可以比较容易恢复。可以使用后面介绍的数据恢复软件轻松地把误删除或意外丢失的文件找回来。不过特别注意的是，在发现文件丢失后，准备使用恢复软件时，千万不要在本机安装这些恢复工具，因为软件的安装可能恰恰把刚才丢失的文件覆盖掉。最好使用能够从光盘直接运行的数据恢复软件，或者把硬盘挂在别的机器上进行

恢复。

特别是文件存储在C盘的情况下，如果发现主要文件被误删除或意外丢失时，这时应该立即关闭电源，用软盘启动进行恢复或把硬盘挂接到其机器上进行处理。

误格式化的情况可以使用UNFORFAT或EasyRecovery等工具进行处理。但是如果使用的是Format X:/U命令进行的格式化，那么这种情况是无法恢复的。

4. 数据恢复范围

1) 误操作类

误删除、误格式化、误分区、误克隆等。

2) 破坏类

病毒分区表破坏、病毒FAT、BOOT区破坏、病毒引起的部分DATA区破坏。

3) 软件破坏类

Format、Fdisk、IBM-DM、PartitionMagic和Ghost等(注：冲零或低级格式化后的硬盘将无法修复数据)。

4) 硬件故障类

0磁道损坏、硬盘逻辑锁、操作时断电、硬盘芯片烧毁、软盘/光盘/硬盘无法读盘。

5) 加密解密

Zip、Rar、Office文档、Windows 2000/XP系统密码。

5. 彻底删除文件的方法

那么，如何让被删除的文件无法恢复呢？如果将文件删除后重新写入新数据，反复多次后原始文件就可能找不回了。但操作起来比较麻烦，而且也不够保险。因此最好能借助一些专业的删除工具来处理，例如O&O SafeErase可以设置5种删除级别，默认的Highest Security(最高级别的安全删除)算法将使用预设规则重写数据35次，可让原始数据变得“面目全非”。

6. 数据恢复软件EasyRecovery简介

EasyRecovery是世界著名数据恢复公司Kroll Ontrack的技术杰作。其Professional版更是囊括了磁盘诊断、数据恢复、文件修复、E-mail修复全部4大类19个项目的各种数据文件修复和磁盘诊断方案。本实验使用的就是EasyRecovery Professioanl，版本为11.1共享版，目前在网上可以很方便地找到。

EasyRecovery在修复过程中不对原数据进行改动，只是以读的形式处理要修复的分区。它不会将任何数据写入它正在处理的分区。EasyRecovery可运行于Windows 95、98、NT、2000以及XP，并且它还包括了一个实用程序用来创建紧急启动软盘，以便在不能启动进入Windows的时候在DOS下修复数据。

EasyRecovery修复范围：

- 修复主引导扇区(MBR)；
- 修复BIOS参数块(BPB)；

- 修复分区表；
- 修复文件分配表(FAT)或主文件表(MFT)；
- 修复根目录；
- 受病毒影响；
- 格式化或分区；
- 误删除；
- 由于断电或瞬间电流冲击造成的数据毁坏；
- 由于程序的非正常操作或系统故障造成的数据毁坏。

3.1.6 实验设备

主流配置 PC 一台，要求安装 Windows 7 操作系统，数据恢复软件 EasyRecovery11.1。

3.1.7 实验步骤

(1) 从指导老师处得到数据恢复软件 EasyRecovery。

(2) 安装软件。

(3) 运行数据恢复软件 EasyRecovery，如图 3-1-1 所示。

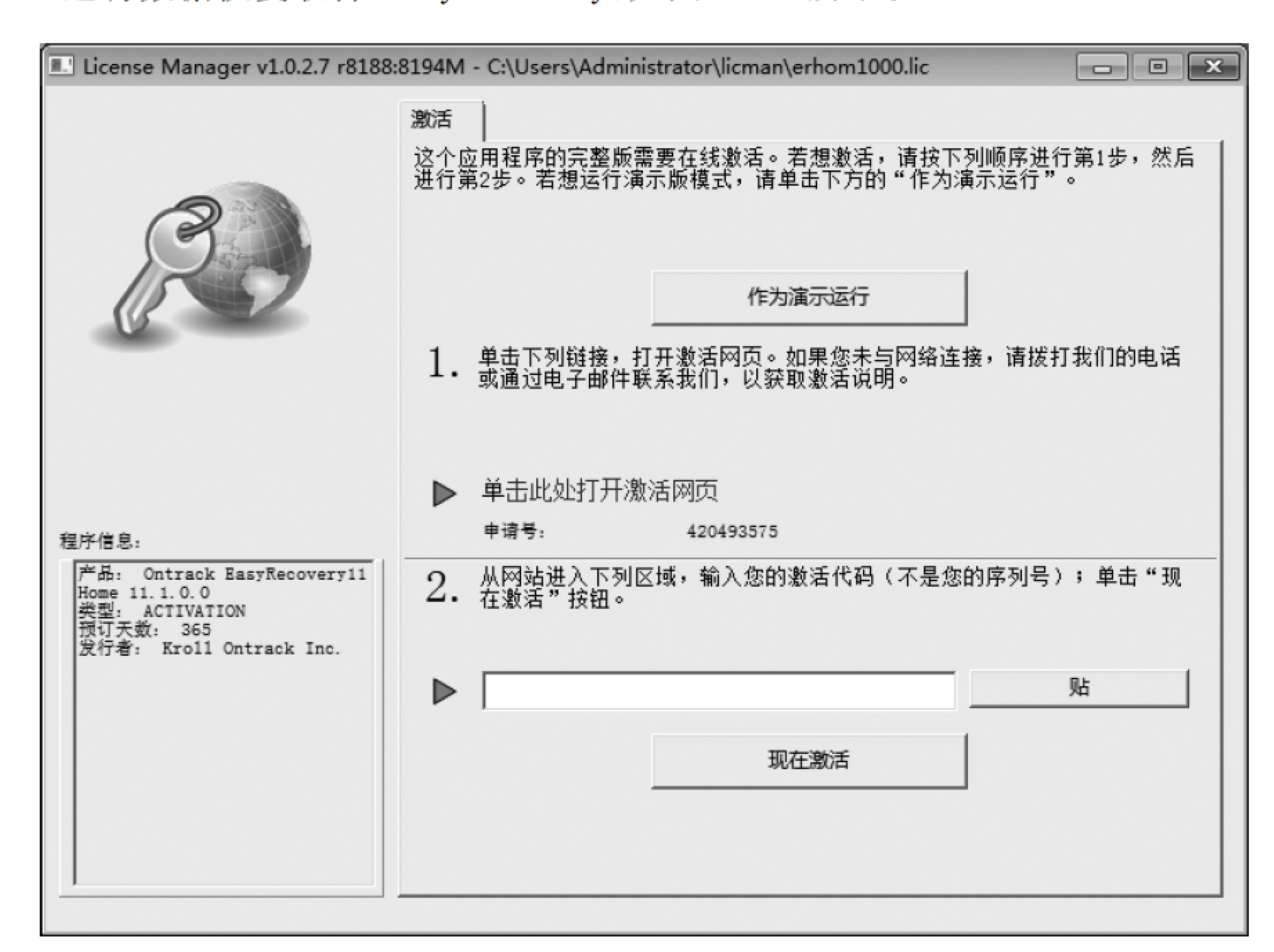


图 3-1-1 启动界面

单击“作为演示运行”按钮，如图 3-1-2 所示。

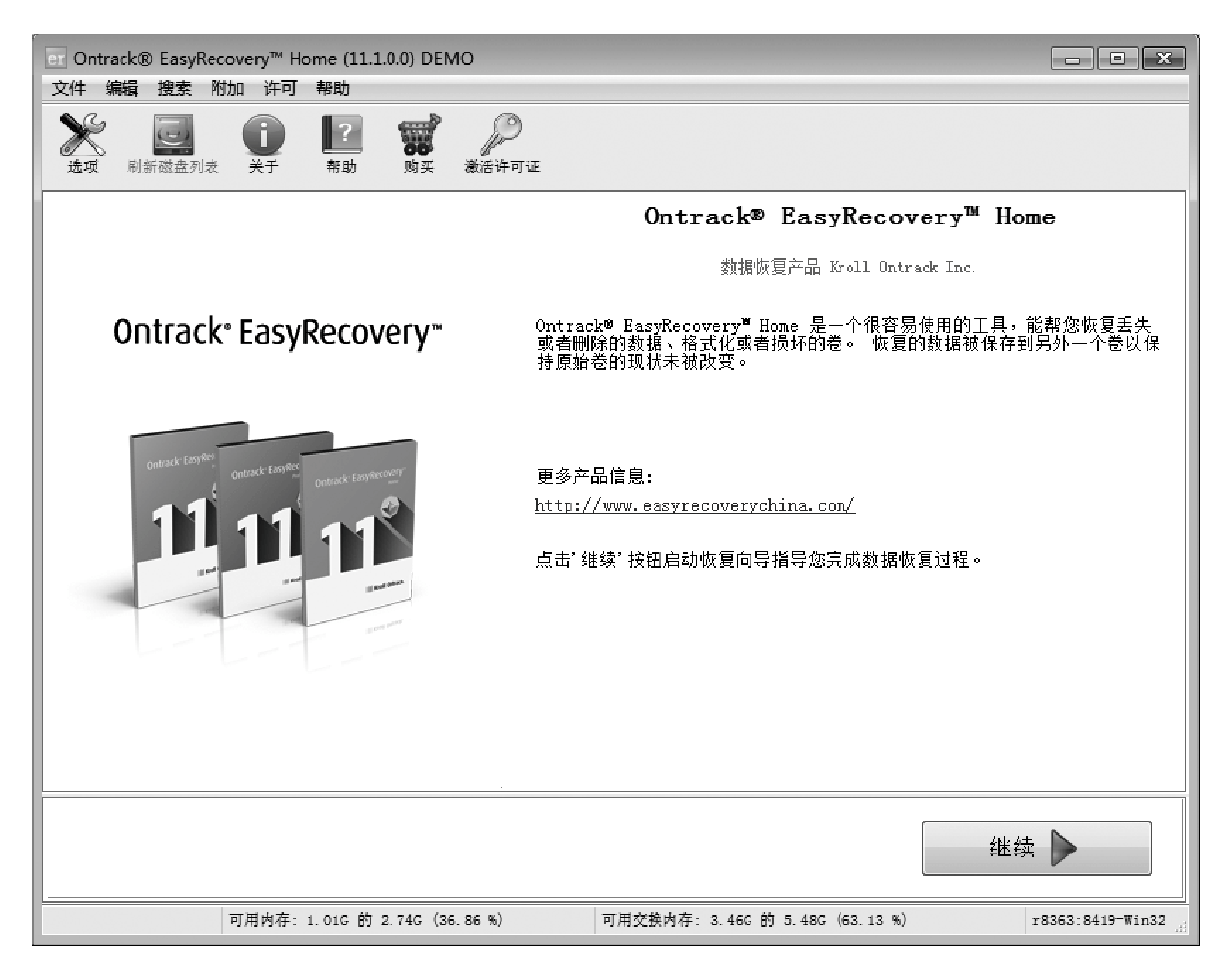


图 3-1-2　单击“作为演示运行”按钮后的界面

单击“继续”按钮，如图 3-1-3 所示。



图 3-1-3　单击“继续”后进入软件数据恢复界面

① 硬盘驱动器：从内部硬盘或其他大容量存储设备中恢复数据；

② 存储设备：从闪盘或其他移动闪存媒体恢复数据；

③ 光学媒体：从光学媒体如CD、CD-R/W、DVD、DVD-R/W等；

④ 多媒体/移动设备：从多媒体或移动设备中恢复数据，如数码相机、MP3、智能电话等；

⑤ RAID系统：恢复RAID系统的数据。

(4) 在E盘根目录，创建文件“密件.txt”，内容为“密码：123456”，并将其复制到优盘，然后删除该文件。

(5) 将优盘插入到USB接口，并双击桌面的快捷方式 Ontrack EasyRecovery Professional，启动数据恢复软件。

(6) 进入到数据恢复界面，选择“存储设备”，并单击“继续”按钮，如图3-1-4所示。



图3-1-4 软件数据恢复界面中选择“存储设备”

(7) 单击“继续”按钮，如图3-1-5所示。

(8) 单击“继续”按钮，如图3-1-6所示。

(9) 单击“继续”按钮，如图3-1-7所示。

(10) 单击“继续”按钮，如图3-1-8所示。

(11) 文件搜索完成后，如图3-1-9所示。

(12) 找到要恢复的文件“密件.txt”，单击工具栏上的“保存“按钮，如图3-1-10所示。

(13) 并单击“保存”按钮，文件恢复成功。



图 3-1-5 选择要恢复数据的优盘



图 3-1-6 选择恢复数据的类型为“恢复已删除的文件”



图 3-1-7　恢复数据选项核查界面

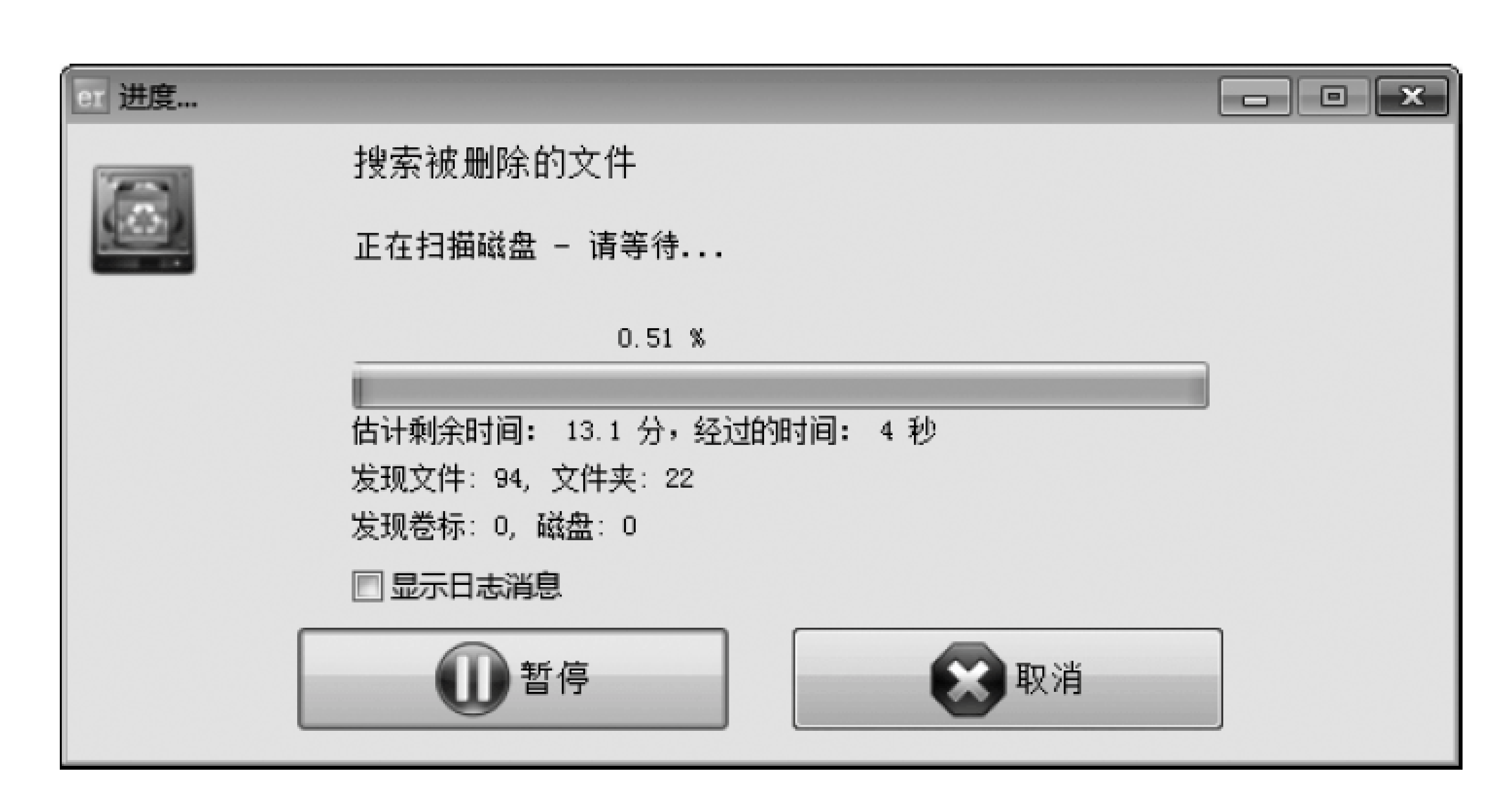


图 3-1-8　数据恢复进度界面

(14) 在桌面上找到“密件.txt”，双击打开文件，如图 3-1-11 所示。

3.1.8　实验思考

(1) 为什么删除的磁盘文件能够恢复回来？

(2) 怎样才能彻底地删除文件？如何使用 GPL 通用公开授权文件删除软件 Eraser 将文件彻底删除？



图 3-1-9 找到需要恢复的文件“密件. txt”



图 3-1-10 选择恢复文件的保存位置



图 3-1-11　发现文件的内容

3.2　操作系统安全评估与检测

3.2.1　实验类型

综合型，4 学时，必选实验。

3.2.2　实验目的

操作系统本身设计的安全性可能比较高，但可能由于使用和配置的不当，造成操作系统实际的安全性能降低。通过操作系统安全评估，发现主机和网络设备的漏洞和安全隐患。通过实验，使学生认识操作系统安全评估与检测的重要性，掌握操作系统安全评估与检测的内容和方法。

3.2.3　题目描述

使用 Windows 基线分析器 MBSA 对操作系统进行安全评估。

3.2.4　实验要求

能够使用 MBSA 实现对本地和远程的 Windows 操作系统实现安全评估。

3.2.5　相关知识

信息系统安全评估过程包括 3 个阶段，分别是文档审查阶段、现场检测阶段和综合评估阶段。评估依据有《信息系统安全保障通用评估准则》及各行业系统评估标准。评估结果以报告的形式给出，通常包括《信息系统安全现场核查报告》、《信息系统安全测试报告》

以及《信息系统安全综合评估报告》等。系统安全评估主要可以划分为操作系统安全评估和应用服务系统安全评估，操作系统的安全评估主要针对操作系统的漏洞、不当的配置，而应用服务的安全评估是针对运行于操作系统之上的软件系统。应用系统安全评估的对象包含非附属于操作系统的软件产品（如数据库、业务系统）提供的各种服务，如 Web 服务、Mail 服务、数据库等应用进行一个全面的安全评估。通过对系统的安全评估，还可以提供针对系统的优化建议和加固服务，使系统和应用能够抵御各种安全威胁。

Windows 系统的"漏洞"就像它的 GUI（图形界面）一样"举世闻名"，几乎每个星期都有新的漏洞被发现。这些漏洞常被计算机病毒和黑客们用来非法入侵计算机，进行大肆破坏。虽然微软会及时发布修补程序，但是发布时间是随机的，而且这些漏洞会因 Windows 软件版本的不同而发生变化，这就使得完全修补所有漏洞成为头号难题。

解决这个难题的简单方法就是利用特定的软件对 Windows 系统进行扫描，检查是否存在漏洞，哪些方面存在漏洞，以便及时修补。

微软开发的免费软件——微软基准安全分析器（Microsoft Baseline Security Analyzer，MBSA），该软件能对 Windows、Office、IIS、SQL Server 等软件进行安全和更新扫描（如表 3-2-1 所示），扫描完成后会用"X"将存在的漏洞标示出来，并提供相应的解决方法指导修补。

表 3-2-1　MBSA 支持的微软产品

产　品　名	安全扫描	更新扫描
Windows Server 2003/XP/2000，NT 4.0	是	是
Exchange Server 5.5 及更高版本	否	是
IIS 4.0 及更高版本	是	是
IE 5.01 及更高版本	是	是
Office 2000 及更高版本	是	是
SQL Server 7.0 及更高版本	是	是
Windows Media Player 6.4 及更高版本	否	是

MBSA 只能在 Windows 2000/XP/2003 系统上运行。在微软的官方网站上可以下载到最新版的 MBSA，而且只需要按照"安装向导"的提示操作即可完成安装过程。安装完成后，依次单击"开始"→"程序"→Microsoft Baseline Security Analyzer 1.2.1 程序项（或双击"桌面"上的 Microsoft Baseline Security Analyzer 1.2.1 快捷图标），就可弹出 MBSA 的主窗口。

3.2.6　实验设备

主流配置 PC 一台，Windows 2000 操作系统，Windows 基线分析器 MBSA。

3.2.7 实验步骤

(1) 单击 MBSA 主窗口中的 Scan a computer(或 Pick a computer to scan)菜单，将弹出 Pick a computer to scan 对话框，如图 3-2-1 所示。

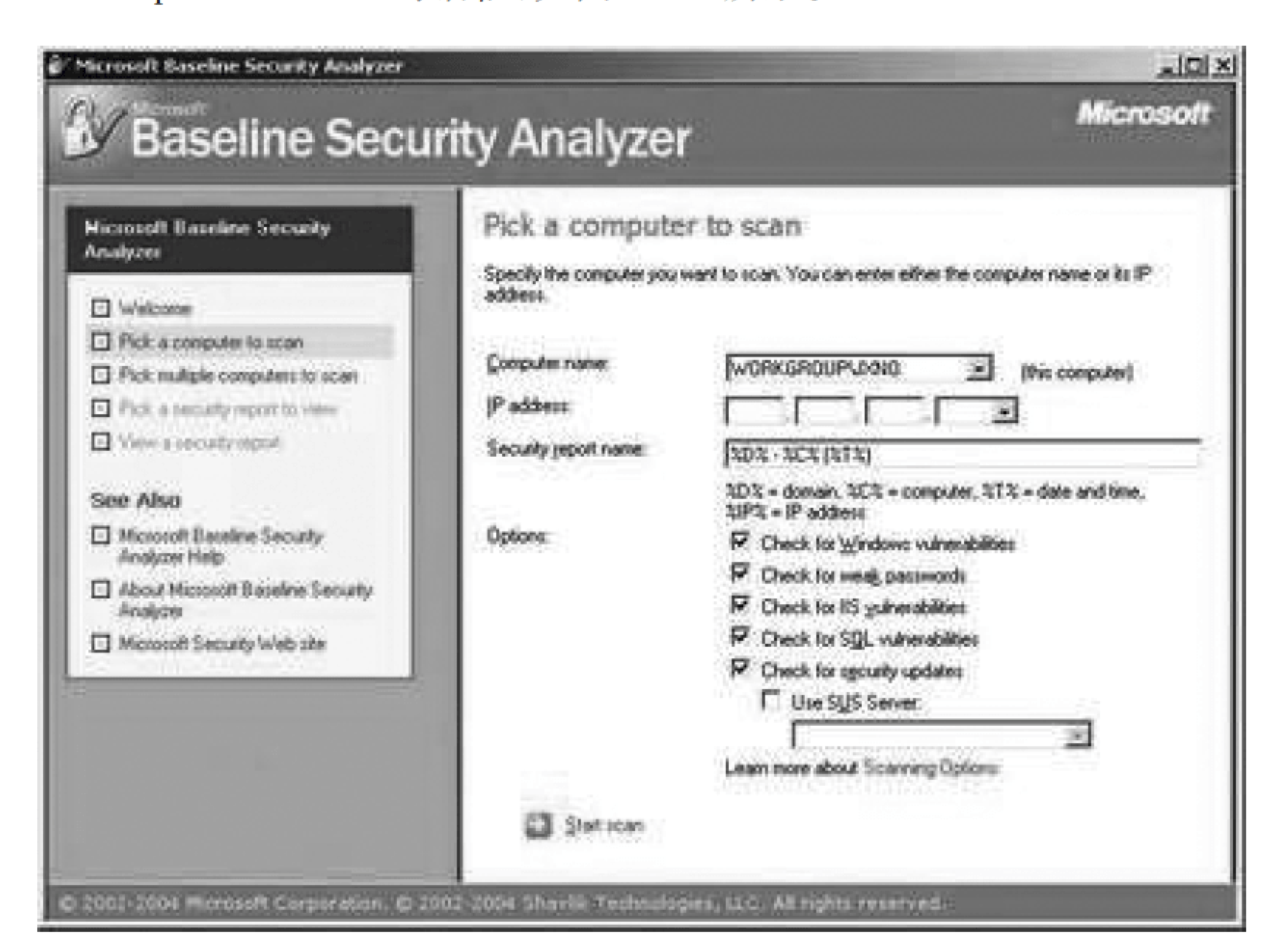


图 3-2-1 选择被扫描的计算机

要想让 MBSA 成功扫描计算机，需在此对话框中进行正确的参数设置。

(2) 设定要扫描的对象。

告诉 MBSA 要扫描的计算机是扫描成功的基础。MBSA 提供两种方法。

方法 1：在 Computer name 文本框中输入计算机名称，格式为“工作组名\计算机名”。

在默认情况下，MBSA 会显示运行 MBSA 的计算机的名称，“WORKGROUP”是所运行 MBSA 的计算机所属的工作组名称，“JXNO”是计算机名称。

方法 2：在 IP address 文本框中输入计算机的 IP 地址。在此文本框中允许输入在同一个网段中的任意 IP 地址，但不能输入跨网段的 IP，否则会提示 Computer not found.(计算机没有找到)的信息。

(3) 设定安全报告的名称格式。

每次扫描成功后，MBSA 会将扫描结果以“安全报告”的形式自动地保存起来。MBSA 允许自行定义安全报告的文件名格式，只要在 Security report name 文本框中输入文件格式即可。

MBSA 提供两种默认的名称格式："%D%-%C%(%T%)"(域名-计算机名(日期戳))和"%D%-%IP%(%T%)"(域名-IP 地址(日期戳))。

(4) 设定扫描中要检测的项目。

MBSA 允许检测包括 Office、IIS 等在内的多种微软软件产品的漏洞。在默认情况下,无论计算机是否安装了以上软件,MBSA 都要检测计算机上是否存在以上软件的漏洞。这不但浪费扫描时间,而且影响扫描速度。可以根据实际情况进行选择,对于一些没有安装的软件可以不选,例如:若没有安装 SQL Server,则可不选中 Check for SQL vulnerabilities 复选项,这样能缩短扫描时间,提高扫描速度。

基于这点考虑,MBSA 提供了让用户自主选择检测项目的功能。只要选中(或取消)Options 中某个复选项,就可让 MBSA 检测(或忽略)该项目。

不过,允许自主选择的项目只有 Check for Windows vulnerabilities(检查 Windows 的漏洞)、Check for weak passwords(检查密码的安全性)、Check for IIS vulnerabilities(检查 IIS 系统的漏洞)、Check for SQL vulnerabilities(检查 SQL Server 的漏洞)等 4 项。

至于其他项目(如 Office 软件的漏洞等)MBSA 会强制扫描。

(5) 设定安全漏洞清单的下载途径。

MBSA 的工作原理是:以一份包含了所有已发现的漏洞的详细信息(如什么软件隐含漏洞、漏洞存在的具体位置、漏洞的严重级别等)的安全漏洞清单为蓝本,全面扫描计算机,将计算机上安装的所有软件与安全漏洞清单进行对比。如果发现某个漏洞,MBSA 就会将其写入到安全报告中。

因此,要想让 MBSA 准确地检测出计算机上是否存在漏洞,安全漏洞清单的内容是否是最新的就至关重要了。

由于新的漏洞不断被发现,所以要像更新防病毒软件的病毒库一样,及时更新安全漏洞清单。MBSA 提供了两种更新方法。

方法 1:从微软官方网站上下载

微软会在它的官方网站上及时发布最新的安全漏洞清单,所以 MBSA 被默认设置为每一次扫描时自动链接到微软官方网站下载最新的安全漏洞清单。如果已经下载了最新的安全漏洞清单,则可取消 Check for security updates 复选项。否则应该选中此复选项,以确保安全漏洞清单的内容是最新的。

此方法适用于能连入 Internet 的计算机。

方法 2:从 SUS 服务器上下载

有些局域网中架设了软件升级服务(Software Update Services,SUS)服务器,所以此类可以选择此方法下载最新的安全漏洞清单,只要选中 Use SUS Server 复选框,并在其下的文本框中输入 SUS 的地址即可。

(6) 根据自身情况设置好各项参数后单击 Start Scan 菜单,将弹出 Scanning 对话框,MBSA 将开始扫描指定的计算机,如图 3-2-2 所示。

(7) 扫描完成后,MBSA 会将扫描的结果以安全报告的形式保存到"X:\Documents and Settings\username\SecurityScans"(X 指 Windows 的系统分区符,username 是操作 MBSA 的人员姓名)文件夹中。此时,MBSA 还会自动弹出 View security report 对话窗,将刚生成的安全报告的内容显示出来,如图 3-2-3 所示。

可以根据安全报告的 Score 列中不同颜色的图标来简单区分被扫描的计算机上哪些

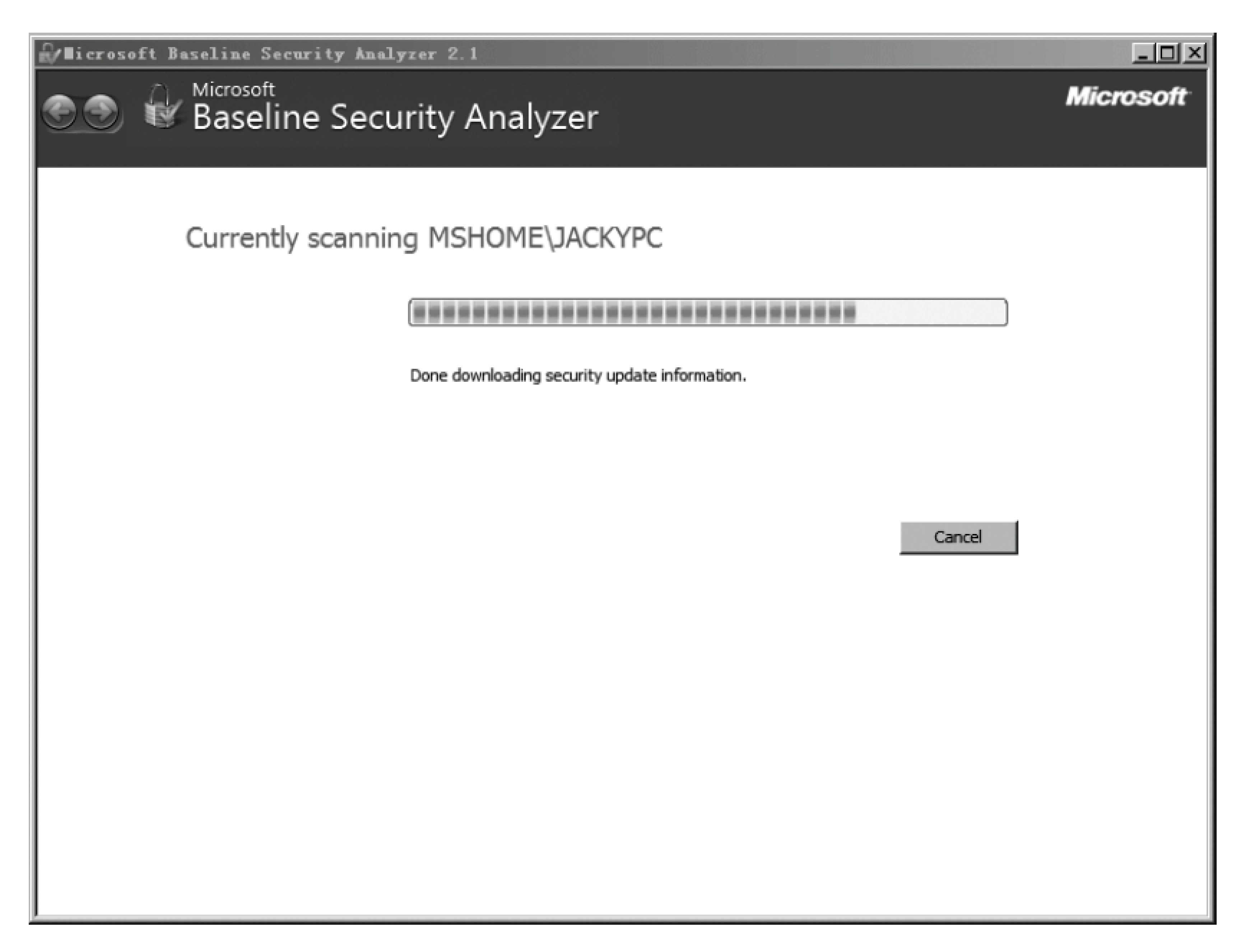


图 3-2-2　扫描过程

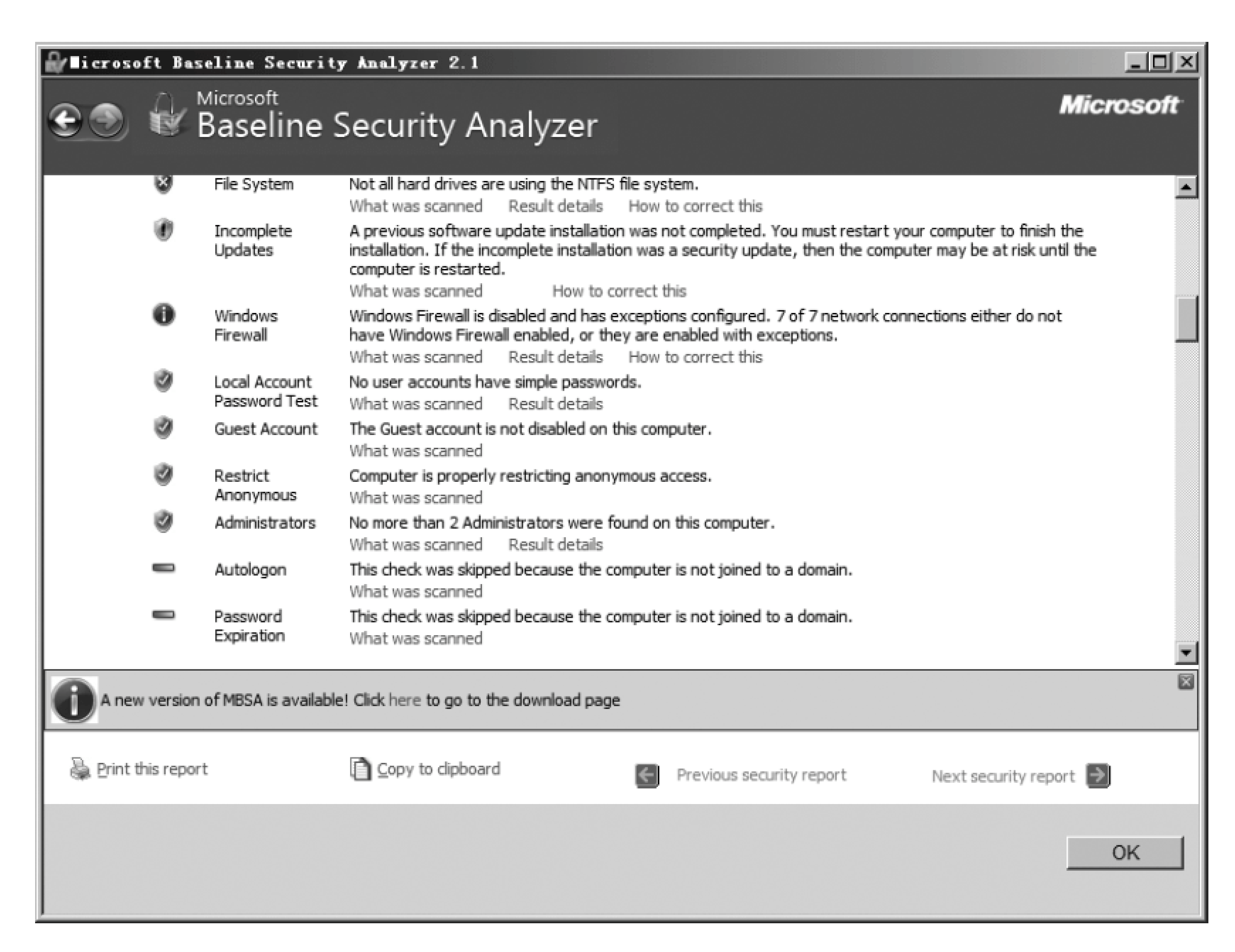


图 3-2-3　扫描结果

方面存在漏洞，哪些方面需要改进，如下所示。

① 绿色的√图标表示该项目已经通过检测。

② 红色(或黄色)的×图标表示该项目没有通过检测，即存在漏洞或安全隐患。

③ 蓝色的 * 图标表示该项目虽然通过了检测但可以进行优化，或者是由于某种原因

MBSA 跳过了其中的某项检测。

④ 白色的 i 图标表示该项目虽然没有通过检测，但问题不很严重，只需要进行简单的修改即可。

但是这种判断方法很不准确，正确的方法是查看检测项目的 Result 列中是否含有 How to correct this（如何修正它）选项。只要有项目存在，就应该单击 How to correct this 选项。然后根据提供的解决方法，或是下载相应的补丁程序，或是修改相关的设置，就可修正存在的问题。

例如：安全报告提示 IE Zones（IE 区域设置）项目没有通过检测，单击 How to correct this 选项后都将弹出信息提示窗（如图 3-2-4 所示），根据 Solution（解决方法）处的文字信息得知，只要按照 Instructions（提示信息）中的步骤更改 IE 的区域设置值即可解决。

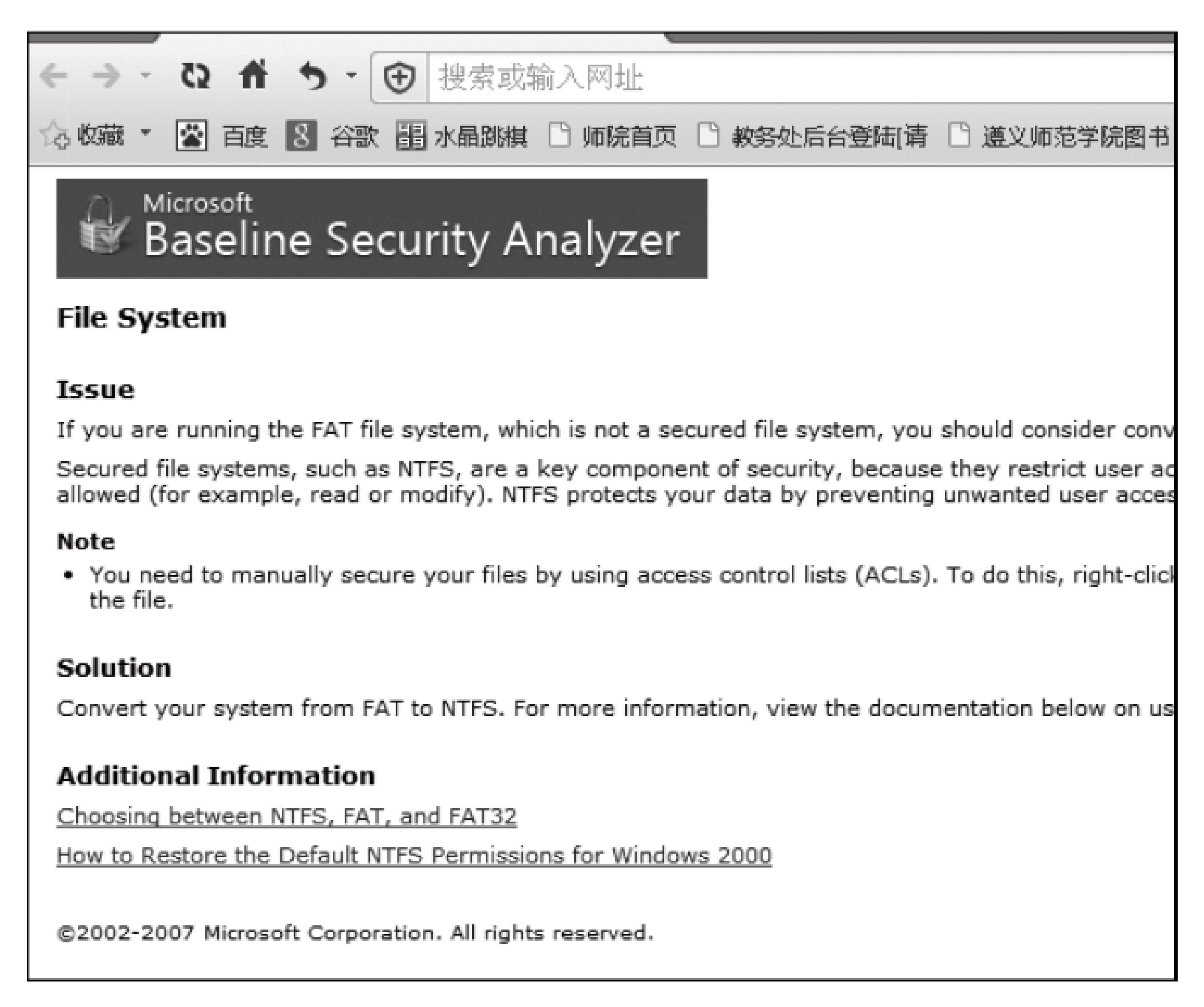


图 3-2-4 提示信息

（8）扫描多台计算机。

此项功能是“扫描一台计算机”功能的延伸，只是将扫描对象扩大到网络中的一个域或 IP 地址段，它的工作原理与“扫描一台计算机”相同，即以安全漏洞清单为蓝本，对指定域（或 IP 地址段）中的所有计算机逐一进行扫描，如图 3-2-5 所示。

注意：*MBSA 只能扫描网络中安装了 Windows NT 4.0/2000/XP/2003 操作系统的计算机，而不能扫描 Windows 9X/Me 系统的计算机。*

具体的操作步骤如下。

第一步：单击 MBSA 主窗口中的 Scan more than one computer（或 Pick multiple computer to scan）菜单，将弹出 Pick multiple computer to scan 对话框。

在此对话框中也要进行必要的、准确的设置。但由于此功能是“扫描一台计算机（Scan a computer）”功能的扩展，所以 Security report name 和 Options 处的设置可以参照操作。

不同的是“指定要扫描的对象”方面：只要在 Domain name 文本框中输入要被扫描的

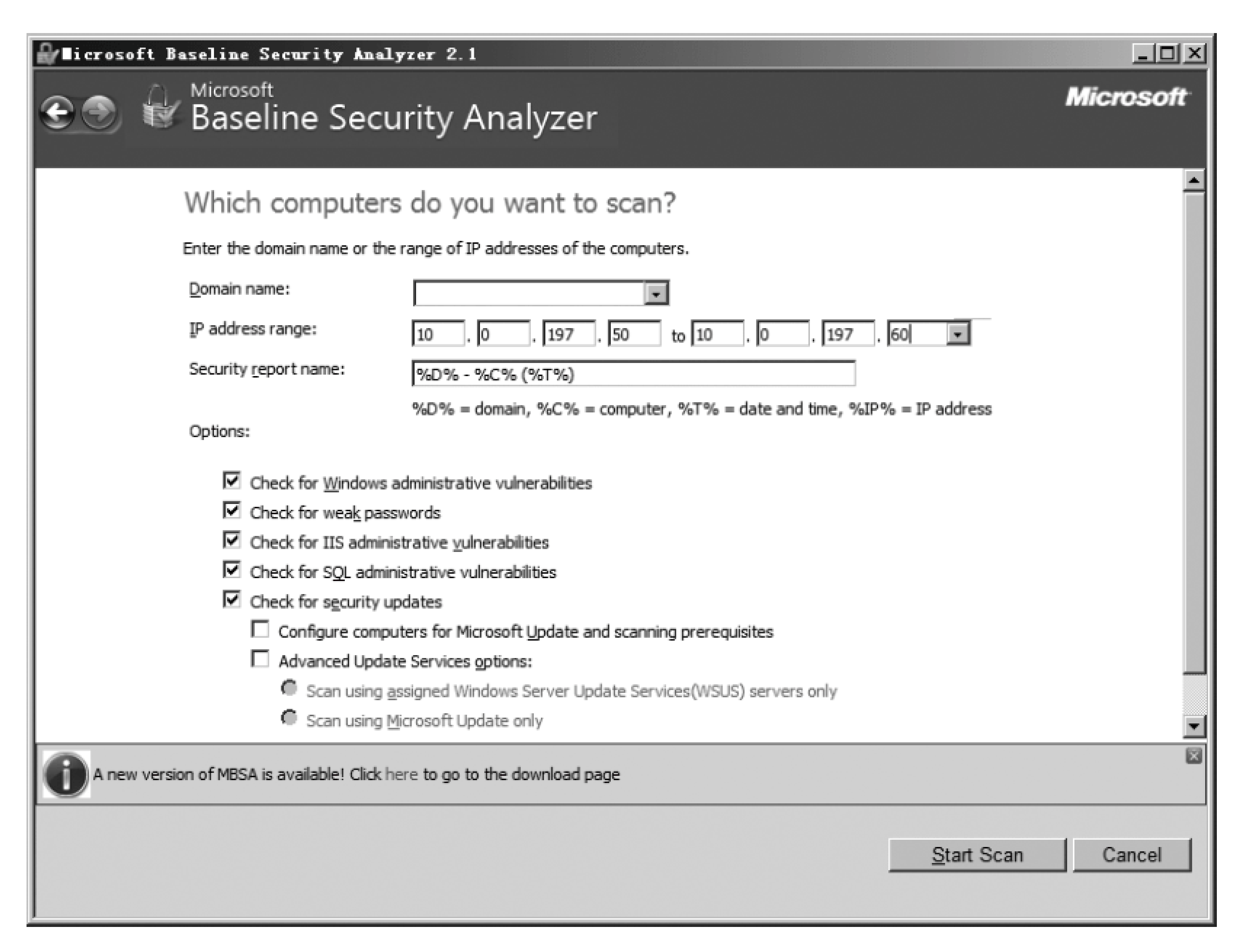


图 3-2-5 扫描多台计算机

域的名称，或在 IP address range 文本框中输入要被扫描的 IP 地址范围，就能让 MBSA 扫描某个域（或 IP 地址段）中的所有计算机。

注意：无论域（或 IP 地址段）中的所有计算机安装的软件是否相同，MBSA 都将依据 Options 处的设置“一视同仁”地扫描每台计算机。

第二步：设定好各项参数后单击 Start Scan 菜单，将弹出 Scanning 对话框，如图 3-2-6

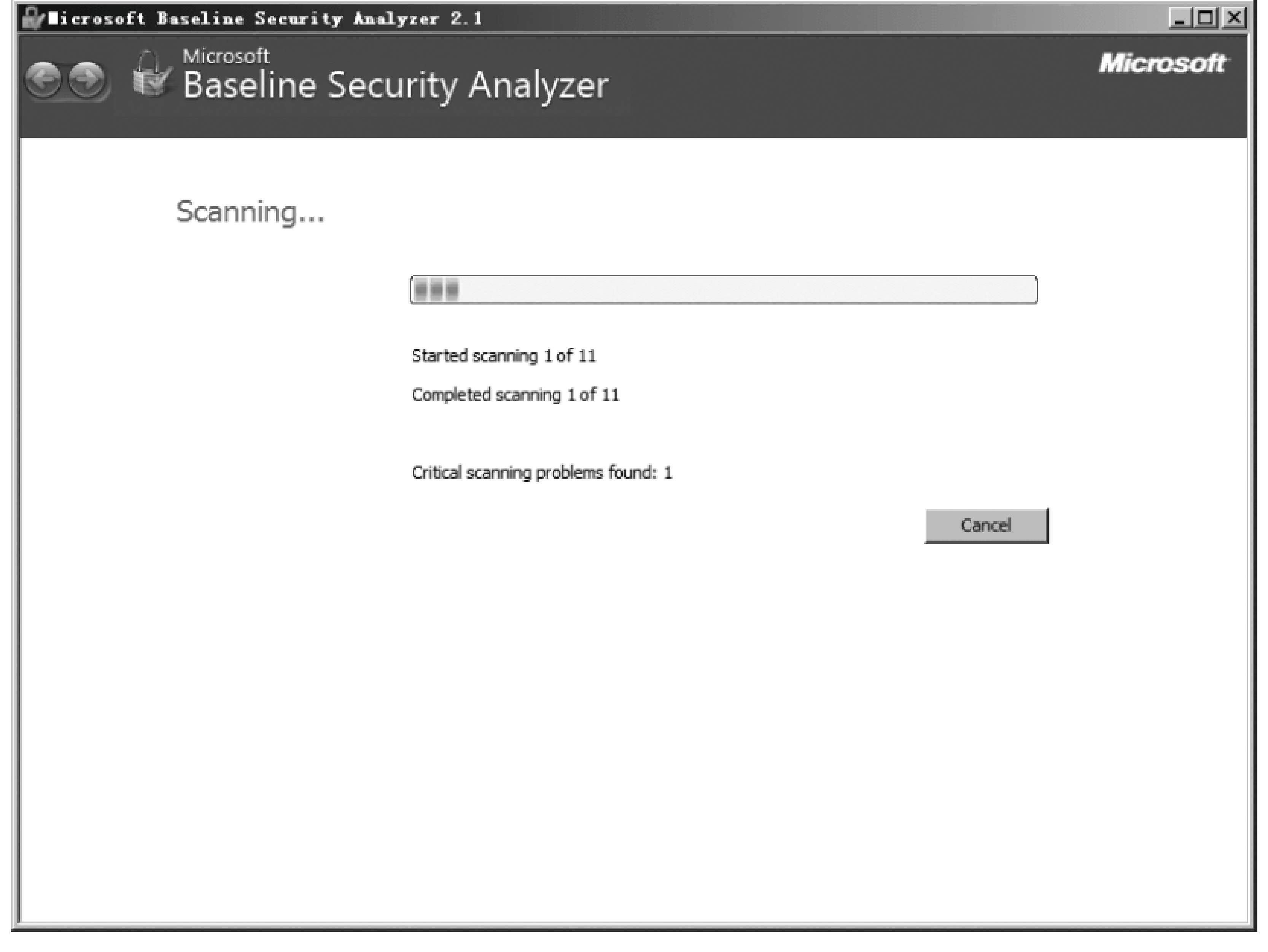


图 3-2-6 扫描过程

所示，MBSA 将依次扫描域(或 IP 地址段)中的每台计算机。完成扫描所需要的时间与被扫描的计算机数量和设置的扫描项目有关。

第三步：与“扫描一台计算机”功能不同的是，扫描结束后，将弹出 Unable to scan all computers 对话框。在此对话框中，将列举没有扫描成功的计算机名(或 IP 地址)及原因。扫描失败的原因有两种，如图 3-2-7 所示。

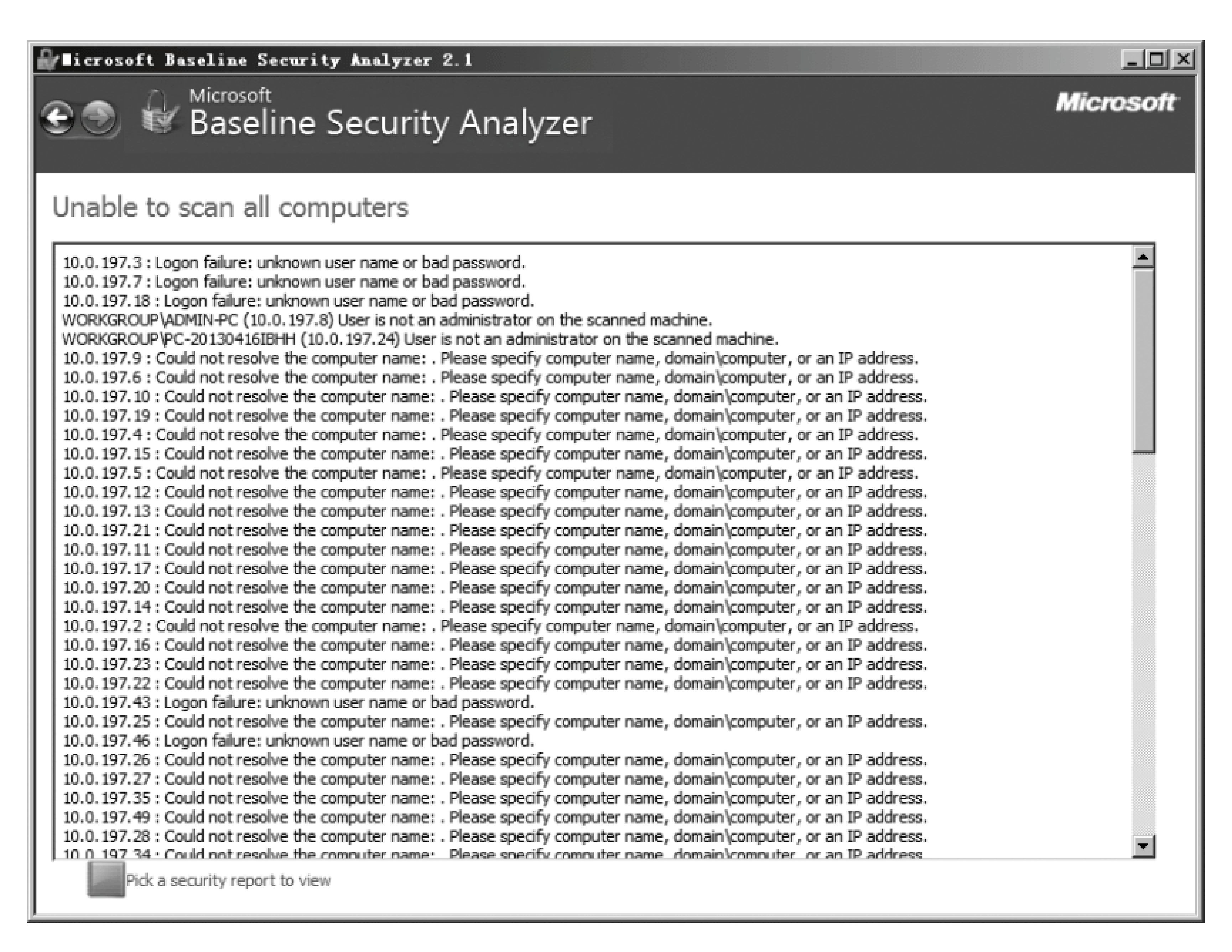


图 3-2-7　出现某些主机不能被扫描

- User is not an administrator on the scanned machine.：被扫描的计算机没有超级管理员权限。

造成这种情况出现的原因主要是没有以 Administrator 的管理员登录操作 MBSA 的计算机或者被扫描的计算机设置了登录密码。

- This is not a Windows NT/2000/XP/2003 Server or Workstation.：被扫描的计算机不是 Windows NT 4.0/2000/XP/2003 系统。

造成这种情况出现的原因是被扫描的计算机没有安装 Windows NT 4.0/2000/XP/2003 操作系统，可能安装了 Windows 9X/Me 系统，或者安装了非 Windows 操作系统，如 Linux 等；或者，被扫描的根本就不是计算机，可能是其他网络设备，如路由器等。

第四步：在 Unable to scan all computers 对话窗的底部还会显示以下菜单之一，以引导进行下一步操作。

- 若显示 Continue 菜单：说明此次扫描中没有一台计算机扫描成功。单击此菜单后将返回到 MBSA 的主窗口。
- 若显示 Pick a security report to view 菜单：说明此次扫描中至少有一台计算机成功地完成扫描并生成了安全报告。单击此菜单后将弹出 Pick a security report to view 对话窗。此时，MBSA 将显示所有扫描成功的计算机的安全报告，供选择

查看其详细内容。

说明：此时无论扫描成功的计算机是几台，MBSA 都不会生成综合性的安全报告，而是为每一台计算机生成各自单独的安全报告。

第五步：选择、查看安全报告。

单击 MBSA 主窗口中的 Pick a security report to view（或 View existing security reports）菜单，将弹出 Pick a security report to view 窗口。在此窗口中，MBSA 将列出已有的所有安全报告清单（包括安全报告名、生成日期等信息），双击安全报告名就可查看其详细内容，如图 3-2-8 所示。

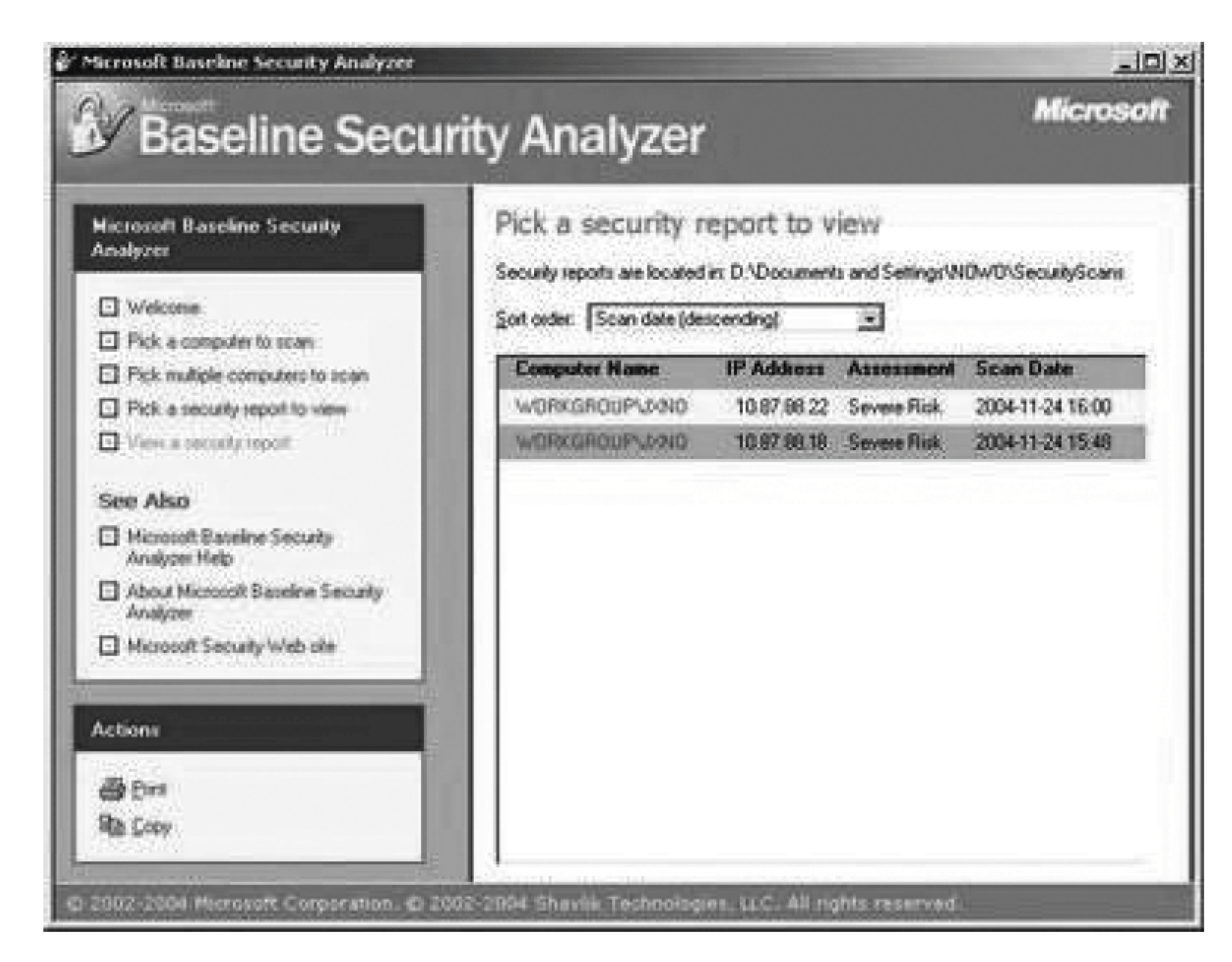


图 3-2-8　扫描结果

安全报告的具体内容、格式、操作方法与“扫描一台计算机”部分的第三步和第四步大同小异，可以参照操作。

(9) 命令行用法。

MBSA 不但能以 GUI 界面运行，还能在命令提示符下运行，执行其安装目录下的 mbsacli.exe 文件就能实现。mbsacli.exe 文件不仅提供了丰富、灵活的参数，而且还支持两种语法结构。

一种是 MBSA 标准的命令行语法结构，即“mbsacli 参数”格式。在命令提示符下运行“mbsacli /?”（仅双引号内的文字）命令可以显示详细的语法信息。另一种是模拟补丁检查工具 HFNetChk 的命令行语法结构，即“mbsacli /hf 参数”格式。运行“mbsacli /hf/?”（仅双引号内的文字）命令可以显示详细的语法信息。

mbsacli.exe 还能用于各种脚本环境中，如命令脚本（.bat 或.cmd 文件）、WSH 脚本（.vbs 或.js 文件）等。通过这些脚本的调用，结合 Windows 系统的其他功能（如“计划任务”功能）就能实现对计算机的灵活扫描。

此外，在MBSA的安装目录下还有两个文本文件，编辑它们就能定制MBSA的扫描过程和方式。

services.txt文件包含了MBSA要扫描的服务（见图3-2-9），默认值为MSFTPSVC、TlntSvr、W3SVC和SMTPSVC服务。添加（或删除）服务名可以让MBSA进行（或忽略）对该服务的检测。



图 3-2-9　扫描的服务

NoExpireOk.txt文件包含了MBSA不扫描的账户名，如IUSR_*、IWAM_*、SUPPORT_*、SQLDebugger等，如图3-2-10所示。删除（或添加）账户名可以让MBSA增加（或忽略）对该账户的检测。

（10）注意事项。

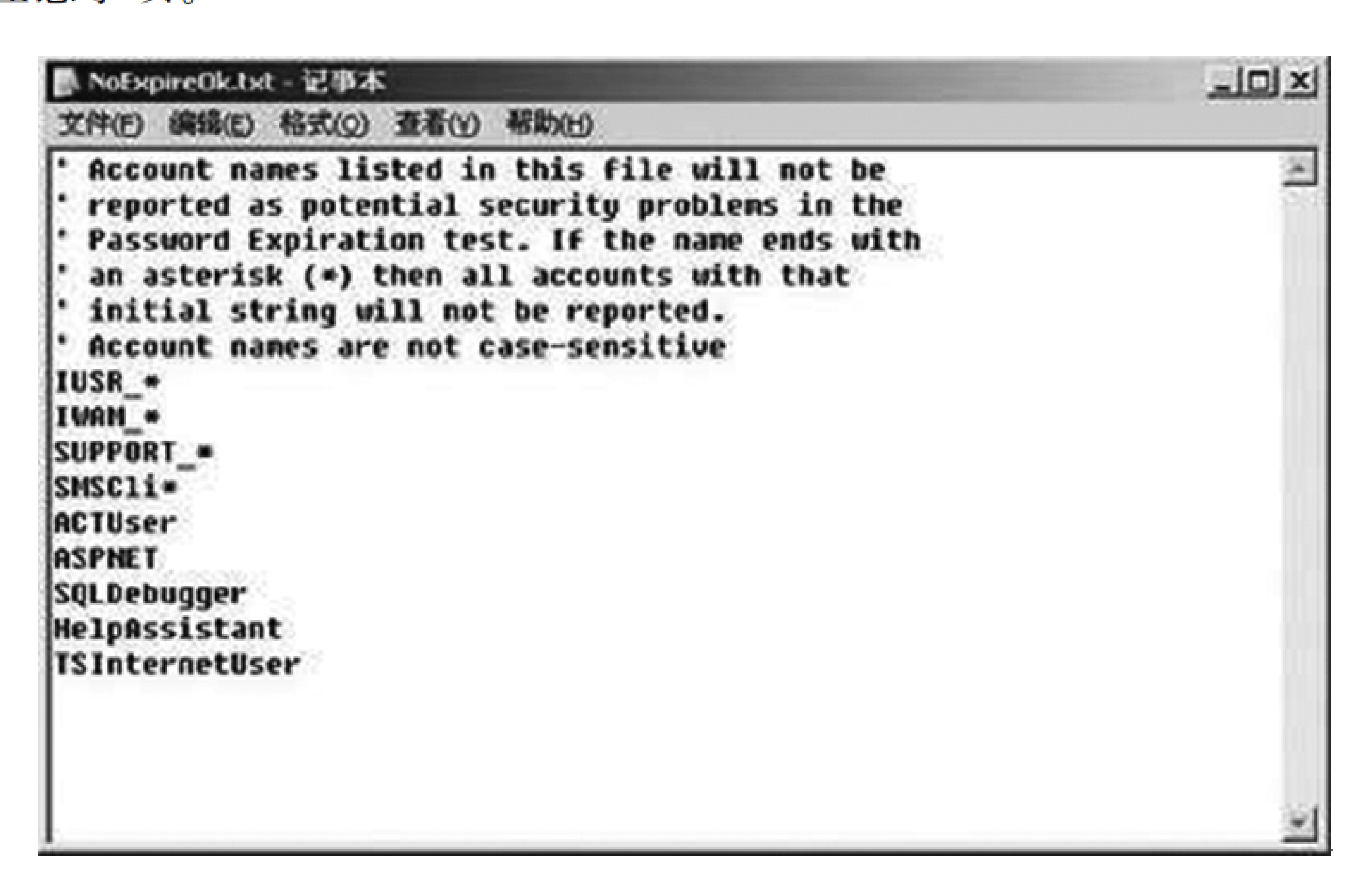


图 3-2-10　扫描的账号

MBSA虽然好用，但是在使用过程中还需要注意以下事项。

① MBSA对Windows、Office、IIS等软件进行的扫描包括以下两种。

- “安全扫描”是指扫描以上软件是否进行了安全的配置，如IIS锁定工具是否已运行，文件系统的类型是否都采用了NTFS格式等。
- “更新扫描”是指扫描以上软件是否安装了最新的补丁程序。

② MBSA执行的是微软所谓的“基准扫描”，即只扫描和报告Windows Update定义的“关键更新”，而不是扫描和报告所有的更新。而且MBSA不会自动安装更新，需要另行操作完成。否则，漏洞依然存在。

③ MBSA是基于IE页面开发的，所以要运行MBSA需要Internet Explorer 5.01以上才行，而且IE的所有设置项都会影响MBSA的运行。

④ 每次扫描后生成的安全报告是以明码格式保存到固定的文件夹中。因此，容易被黑客利用从而找出计算机的漏洞所在。所以建议对安全报告另行处理(如打印、备份到其他目录等)，然后彻底删除SecurityScans文件夹中的所有文件，以防被他人利用。

总之，为了确保计算机系统的安全，除了安装安全防护软件(如杀毒软件、防火墙等)外，及时安装漏洞补丁程序是非常重要的。但怎么才能知道哪些补丁程序还没有安装呢？使用了MBSA就可以知道得一清二楚。而且MBSA具有其他同类软件无法比拟的优点：除了能检查Windows的漏洞，还能检测Office、IIS等微软产品的漏洞。故建议使用Windows 2000/XP/2003的下载该软件，用它检测出计算机中隐含的漏洞和安全隐患，尽早修补，以增强计算机的安全性。

当然，除了MBSA之外，还有很多免费或共享漏洞扫描工具(如HFNetChk、LANguard Network Security Scanner等)，它们的功能也很实用，有兴趣的可以一试。

3.2.8 实验思考

(1) Windows操作系统常见的不安全配置包括哪些方面？

(2) 安全评估与安全检测的区别和联系是什么？

3.3 数据加密与鉴别

3.3.1 实验类型

综合型，8学时，必选实验。

3.3.2 实验目的

密码技术是实现网络信息安全的核心技术，是保护数据最重要的工具之一。密码技术在保护信息安全方面所起的作用体现为保证信息的机密性、数据完整性、验证实体的身份和数字签名的抗否认性。通过实验，使学生掌握古典密码、对称密码体制、非对称密码体制、消息认证、数字签名和信息鉴别等密码算法的特点和密钥管理的原理，能够使用数据加密技术解决相关的实际应用问题，理解密码分析的特点。

3.3.3 题目描述

使用自由软件 dscrypt 完成文件的对称加密和非对称加密操作，使用自由软件 ImageMark 进行数字水印操作，完成经典加密算法替换加密。

3.3.4 实验要求

理解各种常见加密算法的特点，能够使用对称加密、非对称加密软件完成文件的加密操作，能够使用数字水印软件实现数字水印操作。提高要求：能够实现 DES 算法或 RSA 算法。

3.3.5 相关知识

密码技术是信息安全的核心。随着计算机网络不断渗透到各个领域，密码学的应用也随之扩大。数字签名、身份鉴别等都是由密码学派生出来的新技术和应用。

1. 数据加密原理和体制

(1) 数据加密：在计算机上实现的数据加密，其加密或解密变换是由密钥控制实现的。密钥(Keyword)是用户按照一种密码体制随机选取，它通常是一随机字符串，是控制明文和密文变换的唯一参数。

(2) 数字签名、密码技术除了提供信息的加密解密外，还提供对信息来源的鉴别、保证信息的完整和不可否认等功能，而这 3 种功能都是通过数字签名实现的。数字签名的原理是将要传送的明文通过一种函数运算(Hash)转换成报文摘要(不同的明文对应不同的报文摘要)，报文摘要加密后与明文一起传送给接收方，接收方将接收的明文产生新的报文摘要与发送方的发来报文摘要解密比较，比较结果一致表示明文未被改动，如果不一致表示明文已被篡改。

2. 加密体制及比较

根据密钥类型不同将现代密码技术分为两类：一类是对称加密(秘密钥匙加密)系统，另一类是公开密钥加密(非对称加密)系统。对称钥匙加密系统是加密和解密均采用同一把秘密钥匙，而且通信双方都必须获得这把钥匙，并保持钥匙的秘密。

对称密码系统的安全性依赖于以下两个因素。第一，加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；第二，加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性，因此，没有必要确保算法的秘密性，而需要保证密钥的秘密性。对称加密系统的算法实现速度极快，从 AES 候选算法的测试结果看，软件实现的速度都达到了每秒数兆或数十兆比特。对称密码系统的这些特点使其有着广泛的应用。因为算法不需要保密，所以制造商可以开发出低成本的芯片以实现数据加密。这些芯片有

着广泛的应用，适合于大规模生产。

对称加密系统最大的问题是密钥的分发和管理非常复杂、代价高昂。例如对于具有 n 个用户的网络，需要 $n(n-1)/2$ 个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大，分布很广时，密钥的分配和保存就成了大问题。对称加密算法另一个缺点是不能实现数字签名。

公开密钥加密系统采用的加密钥匙（公钥）和解密钥匙（私钥）是不同的。由于加密钥匙是公开的，密钥的分配和管理就很简单，例如对于具有 n 个用户的网络，仅需要 $2n$ 个密钥。公开密钥加密系统还能够很容易地实现数字签名。因此，最适合于电子商务应用需要。在实际应用中，公开密钥加密系统并没有完全取代对称密钥加密系统，这是因为公开密钥加密系统是基于尖端的数学难题，计算非常复杂，它的安全性更高，但它实现速度却远赶不上对称密钥加密系统。在实际应用中可利用二者的各自优点，采用对称加密系统加密文件，采用公开密钥加密系统加密"加密文件"的密钥（会话密钥），这就是混合加密系统，它较好地解决了运算速度问题和密钥分配管理问题。因此，公钥密码体制通常被用来加密关键性的、核心的机密数据，而对称密码体制通常被用来加密大量的数据。

3. 对称密码加密系统

对称加密系统最著名的是美国数据加密标准 DES、AES（高级加密标准）和欧洲数据加密标准 IDEA。

1977 年美国国家标准局正式公布实施了美国的数据加密标准 DES，公开它的加密算法，并批准用于非机密单位和商业上的保密通信。随后 DES 成为全世界使用最广泛的加密标准。加密与解密的密钥和流程是完全相同的，区别仅仅是加密与解密使用的子密钥序列的施加顺序刚好相反。

但是，经过 20 多年的使用，已经发现 DES 很多不足之处，对 DES 的破解方法也日趋有效。AES 将会替代 DES 成为新一代加密标准。

4. 公钥密码加密系统

自公钥加密问世以来，学者们提出了许多种公钥加密方法，它们的安全性都是基于复杂的数学难题。根据所基于的数学难题来分类，有以下三类系统目前被认为是安全和有效的：大整数因子分解系统（代表性的有 RSA）、椭圆曲线离散对数系统（ECC）和离散对数系统（代表性的有 DSA）。

当前最著名、应用最广泛的公钥系统 RSA 是由 Rivet、Shamir、Adelman 提出的（简称为 RSA 系统），它的安全性是基于大整数因子分解的困难性，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法予以解决，因此可以确保 RSA 算法的安全性。RSA 系统是公钥系统的最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。

RSA 方法的优点主要在于原理简单、易于使用。但是，随着分解大整数方法的进步及完善、计算机速度的提高以及计算机网络的发展（可以使用成千上万台机器同时进行大整数分解），作为 RSA 加解密安全保障的大整数要求越来越大。为了保证 RSA 使用的安

全性,其密钥的位数一直在增加,例如,目前一般认为 RSA 需要 1024 位以上的字长才有安全保障。但是,密钥长度的增加导致了其加解密的速度大为降低,硬件实现也变得越来越难以忍受,这对使用 RSA 的应用带来了很重的负担,对进行大量安全交易的电子商务更是如此,从而使得其应用范围越来越受到制约。

DSA(Data Signature Algorithm)是基于离散对数问题的数字签名标准,它仅提供数字签名,不提供数据加密功能。安全性更高、算法实现性能更好的公钥系统椭圆曲线加密算法 ECC(Elliptic Curve Cryptography)基于离散对数的计算困难性。

椭圆曲线加密方法椭圆曲线密码编码学(EllipticCurvesCryptography,ECC)是基于椭圆曲线上离散对数计算问题。椭圆曲线密码体制来源于对椭圆曲线的研究。椭圆曲线加密方法与 RSA 方法相比,有以下优点。

(1) 安全性能更高。

加密算法的安全性能一般通过该算法的抗攻击强度来反映。ECC 和其他几种公钥系统相比,其抗攻击性具有绝对的优势。如 160 位 ECC 与 1024 位 RSA、DSA 有相同的安全强度。而 210 位 ECC 则与 2048bit RSA、DSA 具有相同的安全强度。

(2) 计算量小,处理速度快。

虽然在 RSA 中可以通过选取较小的公钥(可以小到 3)的方法提高公钥处理速度,即提高加密和签名验证的速度,使其在加密和签名验证速度上与 ECC 有可比性,但在私钥的处理速度上(解密和签名),ECC 远比 RSA、DSA 快得多。因此 ECC 总的速度比 RSA、DSA 要快得多。

(3) 存储空间占用小。

ECC 的密钥尺寸和系统参数与 RSA、DSA 相比要小得多,意味着它所占的存储空间要小得多。这对于加密算法在 IC 卡上的应用具有特别重要的意义。

(4) 带宽要求低。

当对长消息进行加解密时,三类密码系统有相同的带宽要求,但应用于短消息时 ECC 带宽要求却低得多。而公钥加密系统多用于短消息,例如用于数字签名和用于对对称系统的会话密钥传递。带宽要求低使 ECC 在无线网络领域具有广泛的应用前景。

ECC 的这些特点使它必将取代 RSA,成为通用的公钥加密算法。例如 SET 协议的制订者已把它作为下一代 SET 协议中默认的公钥密码算法。

3.3.6 实验设备

主流配置 PC 一台,Windows XP 操作系统,自由软件 dsCrypt、ImageMark。

3.3.7 实验步骤

1. 用 dsCrypt 加密 Word 文件

(1) 运行 dsCrypt 软件。

dsCrypt 是一款绿色加密软件,不需要安装。双击即可弹出图 3-3-1 所示的操作

界面。

(2) 设置加密模式。

单击 dsCrypt 操作界面的 Mode 菜单,会改变 dsCrypt 的操作模式。

(3) 设置密码。

单击 dsCrypt 操作界面的 Pass 菜单,输入对文件加密时所需要的密码。单击 OK 完成加密密码设置,如图 3-3-2 所示。

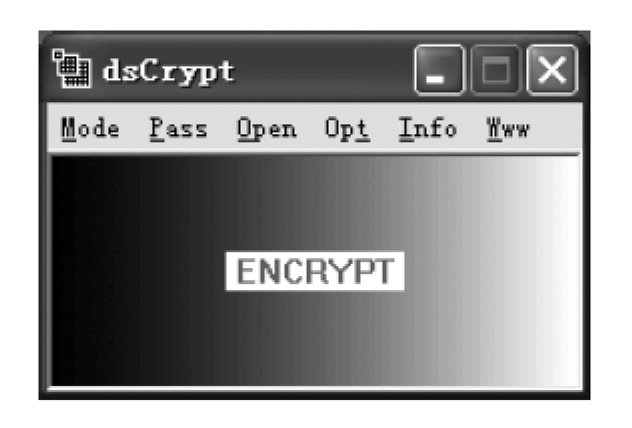


图 3-3-1 运行软件



图 3-3-2 设置密码

(4) 选中保密文件。

单击 dsCrypt 操作界面的 Open 菜单,弹出图 3-3-3 所示的对话框。



图 3-3-3 选择文件

在该对话框中选中要保密的文件,单击“打开”按钮。

可以看出,加密结果是一个扩展名为“.dsc”的加密文件。调用 Word 程序打开该文件时,看到图 3-3-4 所示的结果。

2. 使用 dsCrypt 解密 Word 文件

(1) 运行 dsCrypt 软件。

(2) 设置解密模式。

(3) 设置密码。



图 3-3-4　打开文件显示的内容

单击 Pass 菜单，出现图 3-3-5 所示界面，在该对话框中输入对文件解密时所需要的密码。



图 3-3-5　输入密码对话框

(4) 选中需要解密的文件。

单击 dsCrypt 操作界面的 Open 菜单，在该对话框中选择需要解密的密文文件，然后单击“打开”按钮，如图 3-3-6 所示。



图 3-3-6　选择需要解密文件

解密完成后，调用 Word 程序打开该文件时，可以看到显示结果，如图 3-3-7 所示。

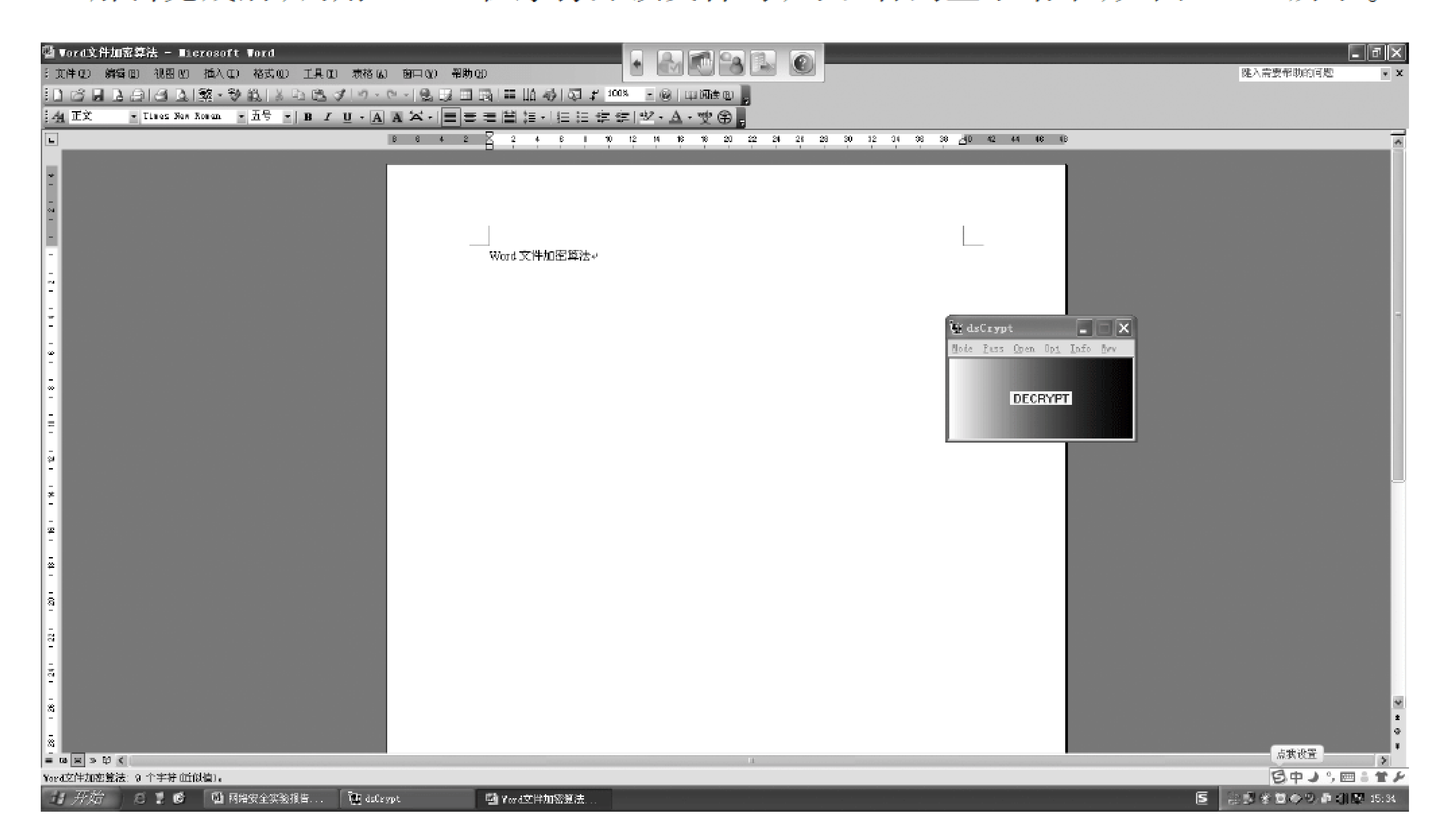


图 3-3-7　解密结果

3.3.8　实验思考

对称加密算法和非对称加密算法在理论和应用上有哪些区别。

3.4　数据库系统安全

3.4.1　实验类型

综合型，4 学时，课外自选实验。

3.4.2　实验目的

当今世界，信息化程度越来越高，大量信息存储在计算机的数据库中，数据库的安全性十分重要。通过该实验，使学生认识数据库系统所面临的安全威胁，了解数据库系统安全的内容，能够使用数据库安全扫描工具进行评估与检测。

3.4.3　题目描述

SQL 注入攻击，SQL Server 2000 新建角色和 Windows 集成身份认证数据库连接，修改 SQL Server 内置存储过程和 SQL 防注入。

3.4.4 实验要求

理解 SQL 注入的原理，掌握安装 SQL Server 2000 并建立数据库，通过 ASP 网页实现 SQL 注入的方法，掌握 SQL Server 2000 角色建立和权限分配方法，掌握 SQL 注入过滤的方法。

3.4.5 相关知识

数据库的应用十分广泛，深入到各个领域，但随之而来产生了数据的安全问题。各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要，关系到企业兴衰、国家安全。因此，如何有效地保证数据库系统的安全，实现数据的保密性、完整性和有效性，已经成为业界人士探索研究的重要课题之一。

(1) 数据库系统的安全除依赖自身内部的安全机制外，还与外部网络环境、应用环境、从业人员素质等因素息息相关，因此，从广义上讲，数据库系统的安全框架可以划分为3个层次：

① 网络系统层次；

② 宿主操作系统层次；

③ 数据库管理系统层次。

这3个层次构筑成数据库系统的安全体系，与数据安全的关系是逐步紧密的，防范的重要性也逐层加强，从外到内、由表及里保证数据的安全。

(2) MS SQL 2000 Server 数据库常见的漏洞。

① sa 弱口令。

存在 Microsoft SQL Server sa 弱口令漏洞的计算机一直是网络攻击者青睐的对象之一，通过这个漏洞，可以轻易地得到服务器的管理权限，从而威胁网络及数据的安全。如 SQL 综合利用工具 SQLTools 和 SQLEXEC。

② SQL 注入漏洞。

利用 ASP 等脚本的漏洞能够进行 SQL 的注入，猜测数据库的内容。

③ 扩展存储过程利用。

利用存储过程 xp_cmdshell 等可以拥有整个系统的控制权限。

④ 另外，MS SQL 2000 Server 本身也存在远程溢出漏洞。

(3) MS SQL 2000 Server 的安全评估。

使用 Microsoft 基线安全性分析器(MBSA)可以评估服务器的安全性。

MBSA 是一个扫描多种 Microsoft 产品的不安全配置的工具，包括 SQL Server 和 Microsoft SQL Server 2000 Desktop Engine(MSDE 2000)。它可以在本地运行，也可以通过网络运行。该工具针对下面问题对 SQL Server 安装进行检测。

① 过多的 sysadmin 固定服务器角色成员。

② 授予 sysadmin 以外的其他角色创建 CmdExec 作业的权利。
③ 空的或简单的密码。
④ 脆弱的身份验证模式。
⑤ 授予管理员组过多的权利。
⑥ SQL Server 数据目录中不正确的访问控制表(ACL)。
⑦ 安装文件中使用纯文本的 sa 密码。
⑧ 授予 guest 账户过多的权利。
⑨ 在同时是域控制器的系统中运行 SQL Server。
⑩ 所有人(Everyone)组的不正确配置,提供对特定注册表键的访问。
⑪ SQL Server 服务账户的不正确配置。
⑫ 没有安装必要的服务包和安全更新。

3.4.6 实验设备

主流配置 PC 一台,Windows 2000 Server 操作系统,MS SQL 2000 Server 数据库软件。

3.4.7 实验步骤

(1) 安装 SQL Server 2000 数据库,SA 密码设置为 123456,过程略。
(2) 安装完成后打开 SQL Server 2000 企业管理器,新建数据库 mydb,如图 3-4-1 所示。

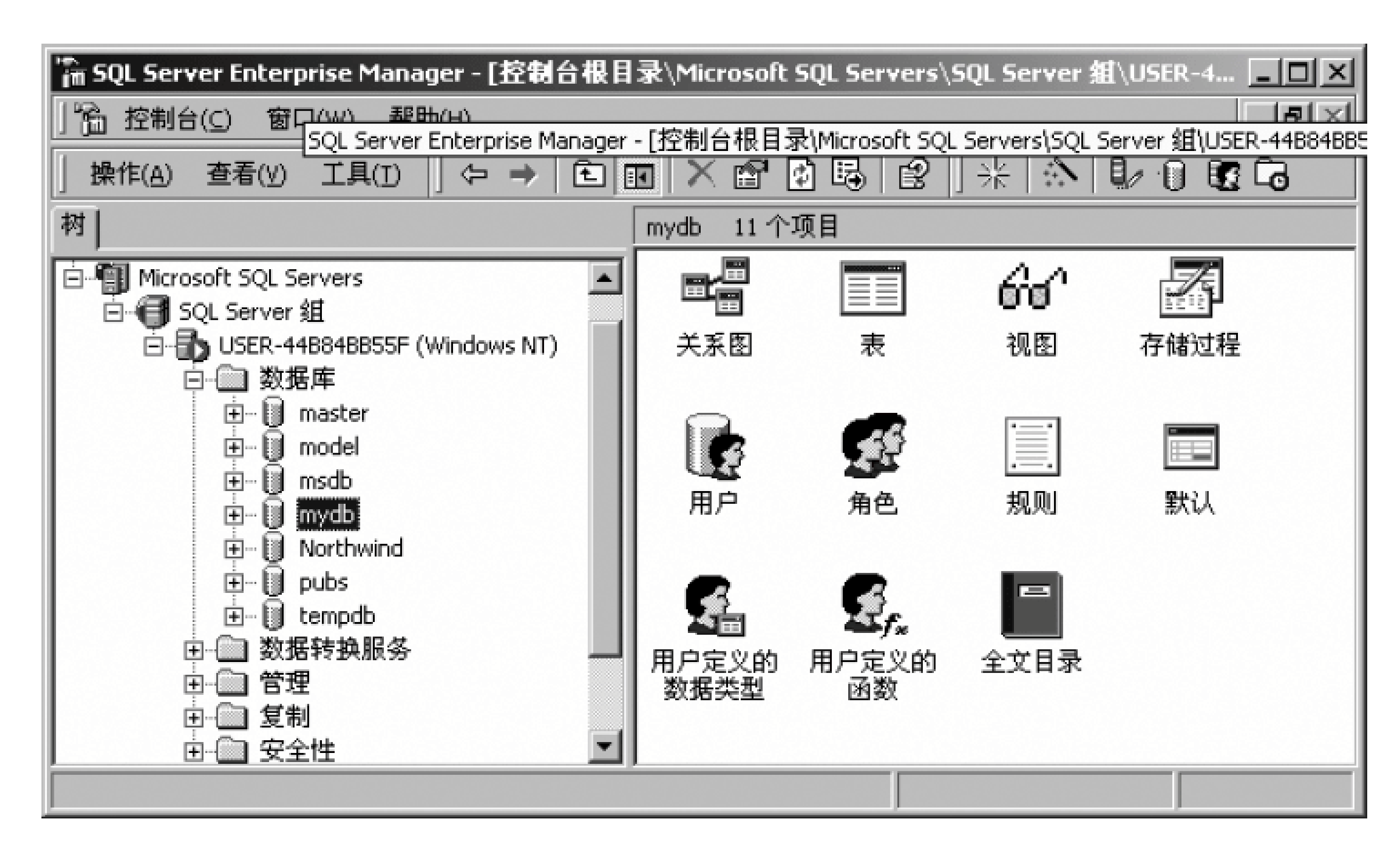


图 3-4-1 新建数据库 mydb

(3) 在 mydb 数据库新建表 mytable,包括 id、name 和 tel 3 个字段。各字段的类型及属性如图 3-4-2 所示。其中 id 字段作为主键和标识。
(4) 在 mytable 表中增加两条记录,如图 3-4-3 所示。
(5) 在 C 盘新建目录 sqltest,并在该目录下新建如下 3 份 ASP 文件。
文件 1:conn.asp

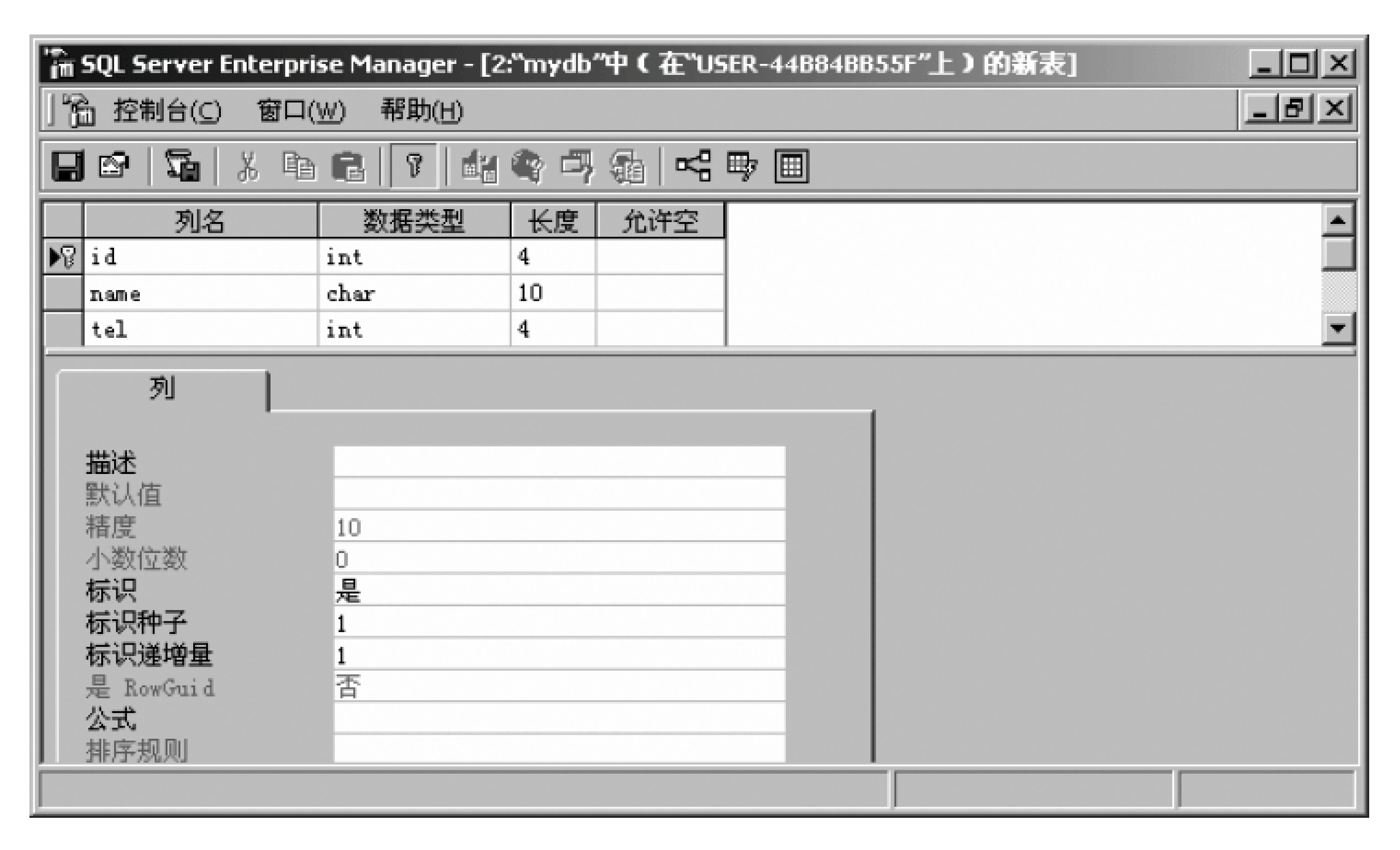


图 3-4-2 新建表 mytable 及字段



图 3-4-3 在 mytable 表中增加两条记录

```
<%
set Conn=Server.CreateObject("ADODB.Connection")
Conn.Open "driver=SQL Server;server=127.0.0.1;uid=sa;pwd=123456;database=mydb;"
%>
```

文件 2：index.asp

```
<!--#include file="conn.asp"-->
<%
set rs=server.createobject("adodb.recordset")
sql="select * from mytable"
rs.open sql,conn,1,1
%>
<table width="100%" border="0" cellspacing="0" cellpadding="0">
<%do while not rs.eof%><tr>
<td><a href="showid.asp?id=<%=rs("id")%>"><%=rs("name")%></a></td>
</tr>
<%
rs.movenext
loop
rs.close
set rs=nothing
conn.close
set conn=nothing
%>
```

```
</table>
```

文件 3：showid.asp

```
<!--#include file="conn.asp"-->
<%
set rs=server.createobject("adodb.recordset")
sql="select * from mytable where id="&request.querystring("id")
rs.open sql,conn,1,1
%>
<html>
<head>
<title>无标题文档</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
</head>
<body bgcolor="#FFFFFF" text="#000000">
<table width="100%" border="0" cellspacing="0" cellpadding="0">
<%
do while not rs.eof
%><tr>
<td><%=rs("name")%></td>
<td><%=rs("tel")%></td>
</tr>
<%
rs.movenext
loop
rs.close
set rs=nothing
conn.close
set conn=nothing
%>
</table>
</body>
</html>
```

(6) 打开 IIS 服务器，将 sqltest 文件夹作为默认目录。

(7) 在浏览器打开 Web 页面。效果如图 3-4-4 所示。

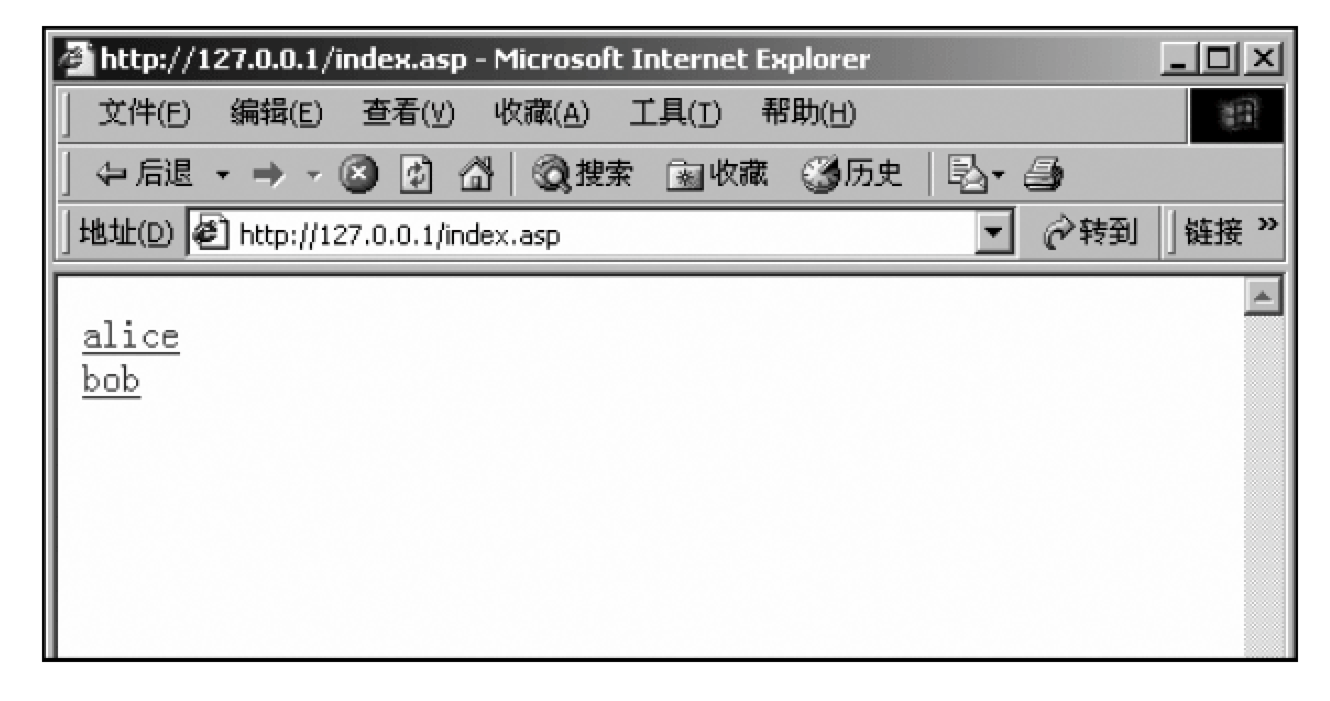


图 3-4-4 浏览器效果

(8) 单击第一条记录,效果如图 3-4-5 所示。

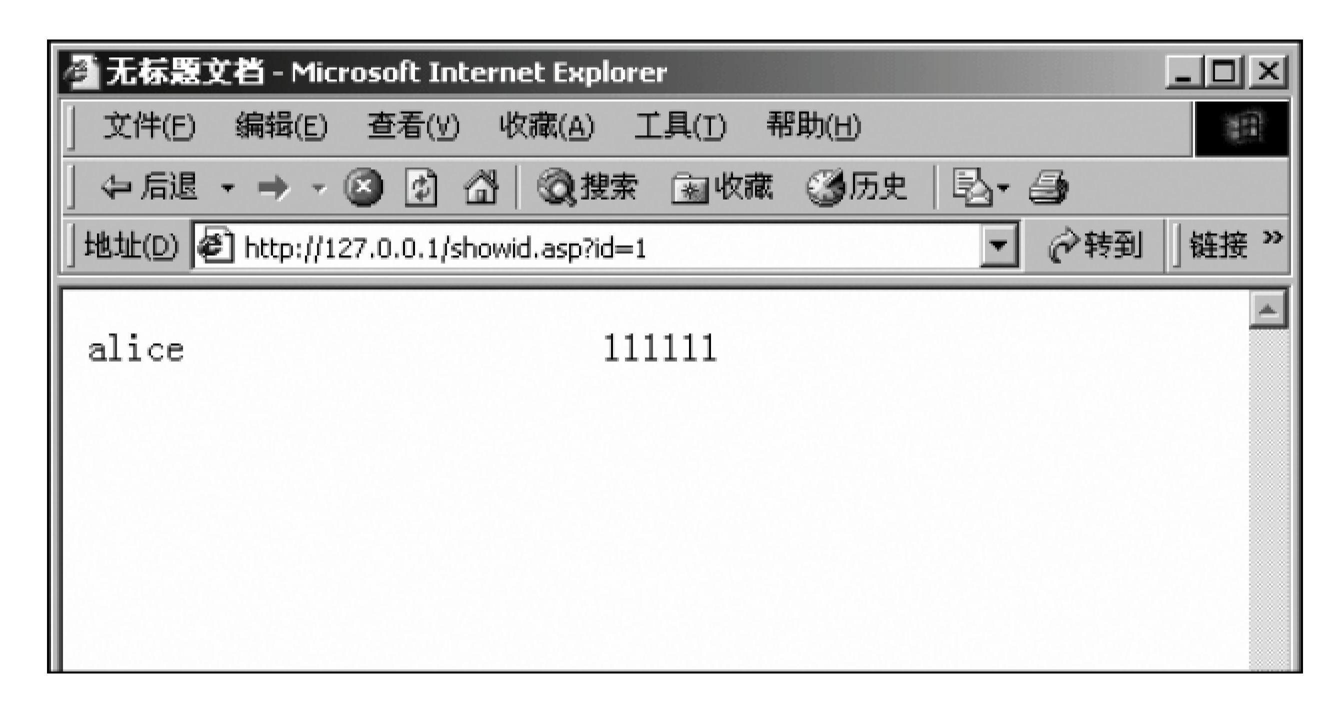


图 3-4-5 浏览器效果

(9) 在地址栏中输入图 3-4-6 所示的内容。

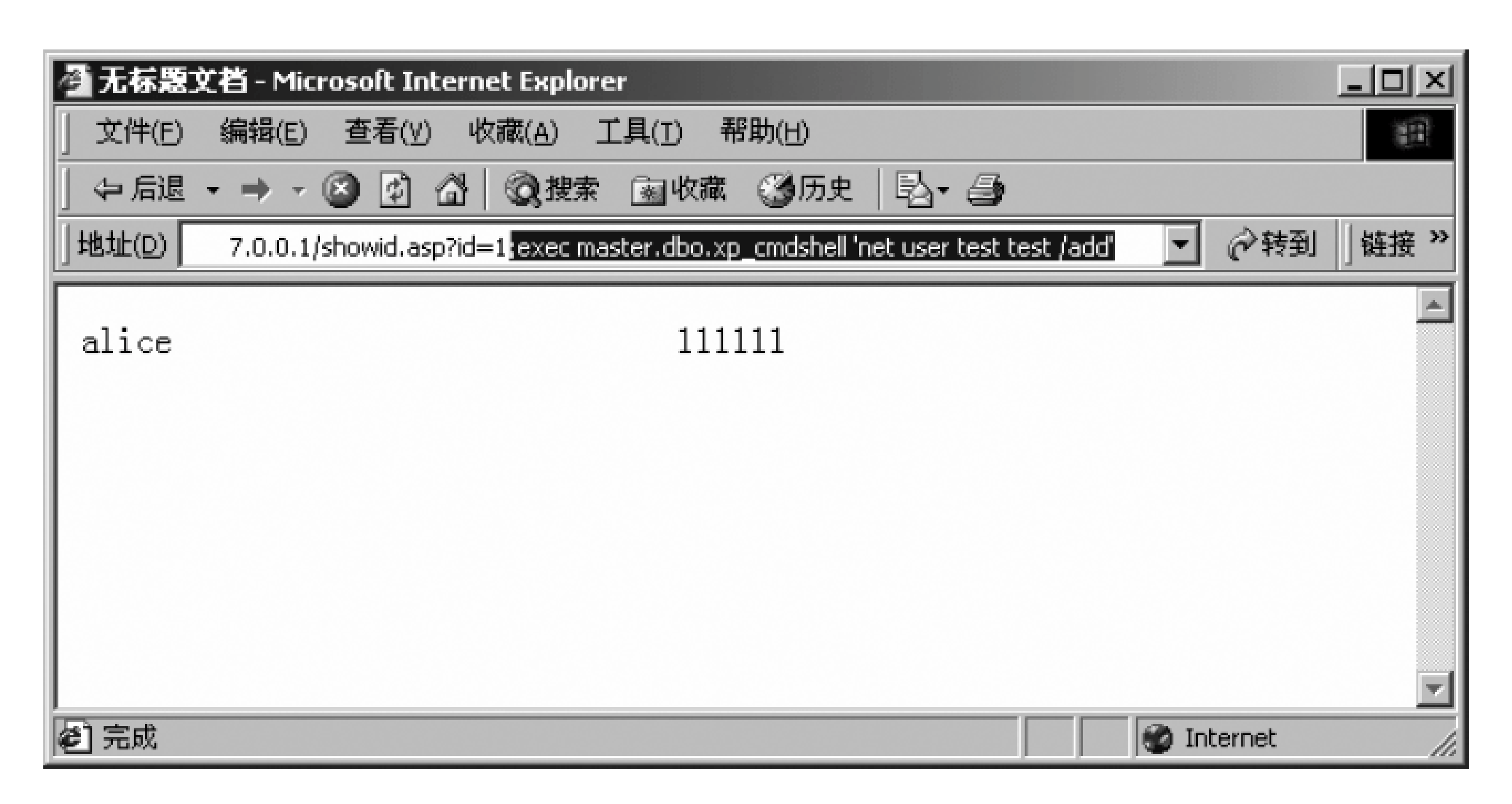


图 3-4-6 注入攻击

(10) 执行结果如图 3-4-7 所示。

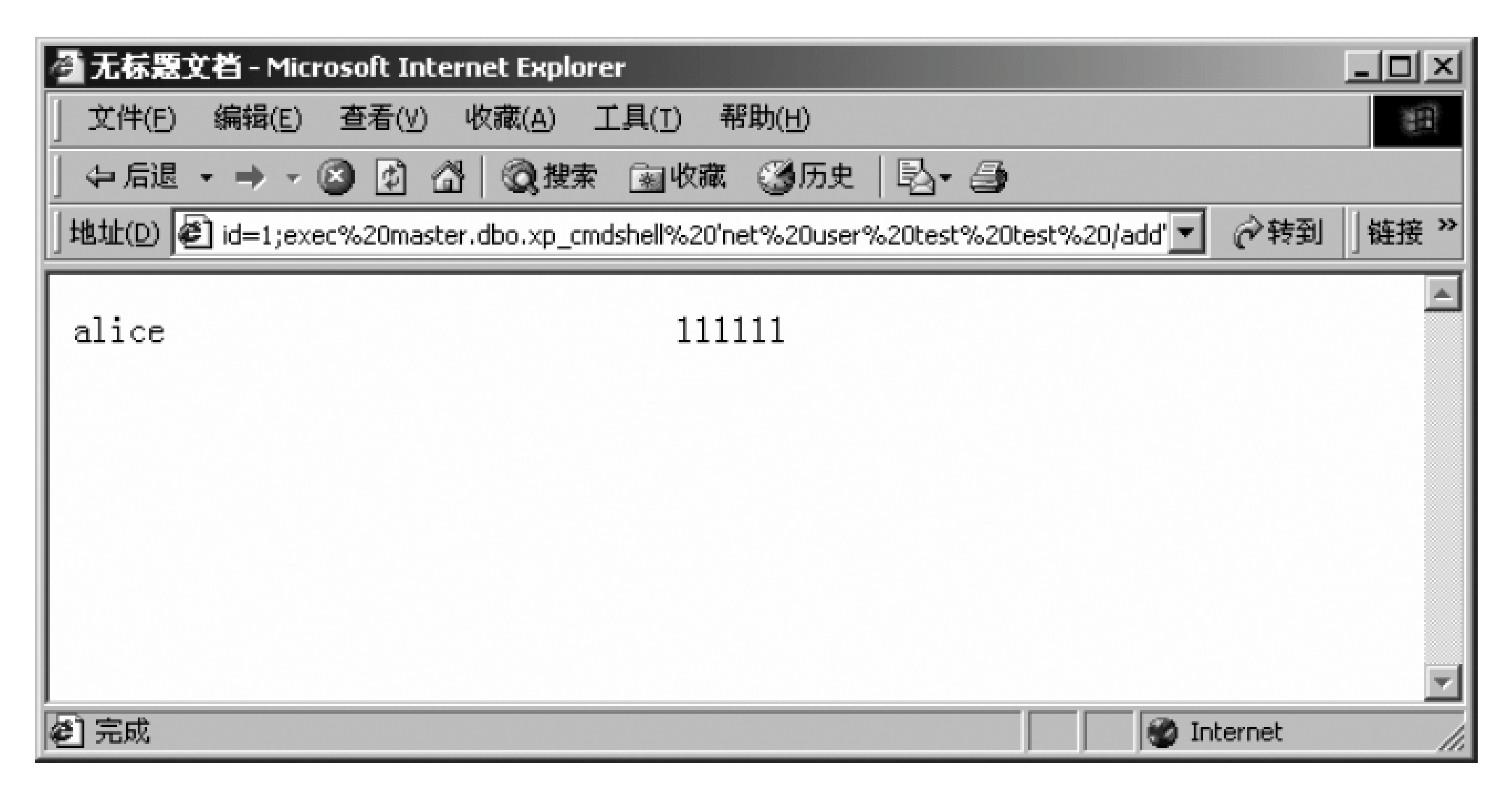


图 3-4-7 攻击结果

(11) 然后查看系统用户,可以发现已经新出现一个账户 test,如图 3-4-8 所示。同样的方法也可以把该账号设置为 administrator 权限。从以上过程可以看到,通过利用 ASP

脚本的注入漏洞和 SQL Server 的不安全配置,能够获得系统的权限。必须采取相应措施以清除注入漏洞并加固数据库系统。



图 3-4-8 用户账户结果

(12) 安装最新的服务包。

为了提高服务器安全性,最有效的一个方法就是升级到 SQL Server 2000 Service Pack 4(SP4)。另外,还应该安装所有已发布的安全更新。

(13) 隔离服务器,并定期备份。

物理和逻辑上的隔离组成了 SQL Server 安全性的基础。驻留数据库的机器应该处于一个从物理形式上受到保护的地方,最好是一个上锁的机房,配备有洪水检测以及火灾检测的消防系统。数据库应该安装在企业内部网的安全区域中,不要直接连接到 Internet。定期备份所有数据,并将副本保存在安全的站点外地点。

(14) 分配一个强健的 sa 密码。

sa 账户应该总拥有一个强健的密码,即使在配置为要求 Windows 身份验证的服务器上也该如此。这将保证在以后服务器被重新配置为混合模式身份验证时,不会出现空白或脆弱的 sa。要分配 sa 密码,按下列步骤操作。

① 展开服务器组,然后展开服务器。

② 展开安全性,然后单击登录,如图 3-4-9 所示。



图 3-4-9 修改密码

③ 在细节窗格中，右击 sa，然后单击属性。

④ 在密码方框中，输入新的密码。

(15) 加强数据库日志的记录。

审核数据库登录事件的“失败和成功”。在实例属性中选择“安全性”，将其中的审核级别选定为全部，这样在数据库系统和操作系统日志里面就详细记录了所有账号的登录事件。定期查看 SQL Server 日志检查是否有可疑的登录事件发生。

(16) SQL Server 的默认安装将监视 TCP 端口 1433 以及 UDP 端口 1434。配置的防火墙来过滤掉到达这些端口的数据包。

(17) 使用 Windows 身份验证方式，为数据库增加 IUSR 用户。

与 SQL Server 身份验证方式相比，Windows 身份验证方式具有下列优点：提供了更多的功能，例如安全确认和口令加密、审核、口令失效、最小口令长度和账号锁定；通过增加单个登录账号，允许在 SQL Server 系统中增加用户组；允许用户迅速访问 SQL Server 系统，而不必使用另一个登录账号和口令。SQL Server 使用 IUSR 用户访问数据库。

展开服务器组，然后展开服务器。展开安全性子项，然后右击“登录”，并单击“新建登录”。在“名称”选择 IUSR 账户，数据库选择 mydb，如图 3-4-10 所示。

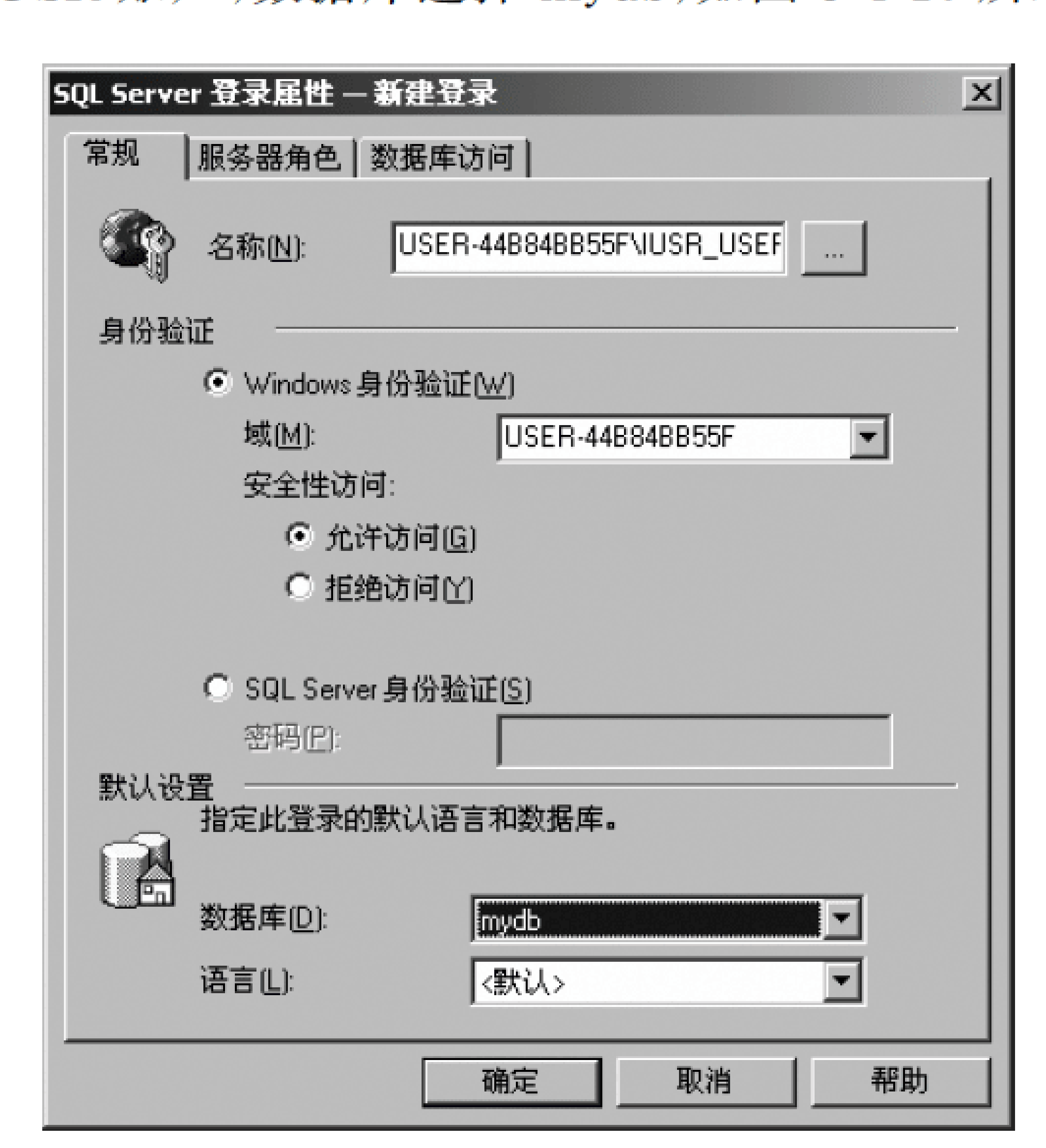


图 3-4-10 新建登录

然后单击“数据库访问”选项卡，按图 3-4-11 所示修改，并单击“确定”，完成数据库访问账户的添加。

(18) 新建角色。通过新建角色创建自己的权限，使数据库的用户拥有合适的权限。避免 SYSADMIN 和 db_owner 的权限过大引起安全问题。

展开“数据库”文件夹，然后展开 mydb 数据库。右击“角色”，然后单击“新建数据库角色”命令。在“名称”框中输入新角色的名称 newjiaose。单击“添加”将成员 IUSR 添加到“标准角色”列表中，并单击确定完成角色的添加，如图 3-4-12 所示。



图 3-4-11　设置新建登录账户访问数据库许可

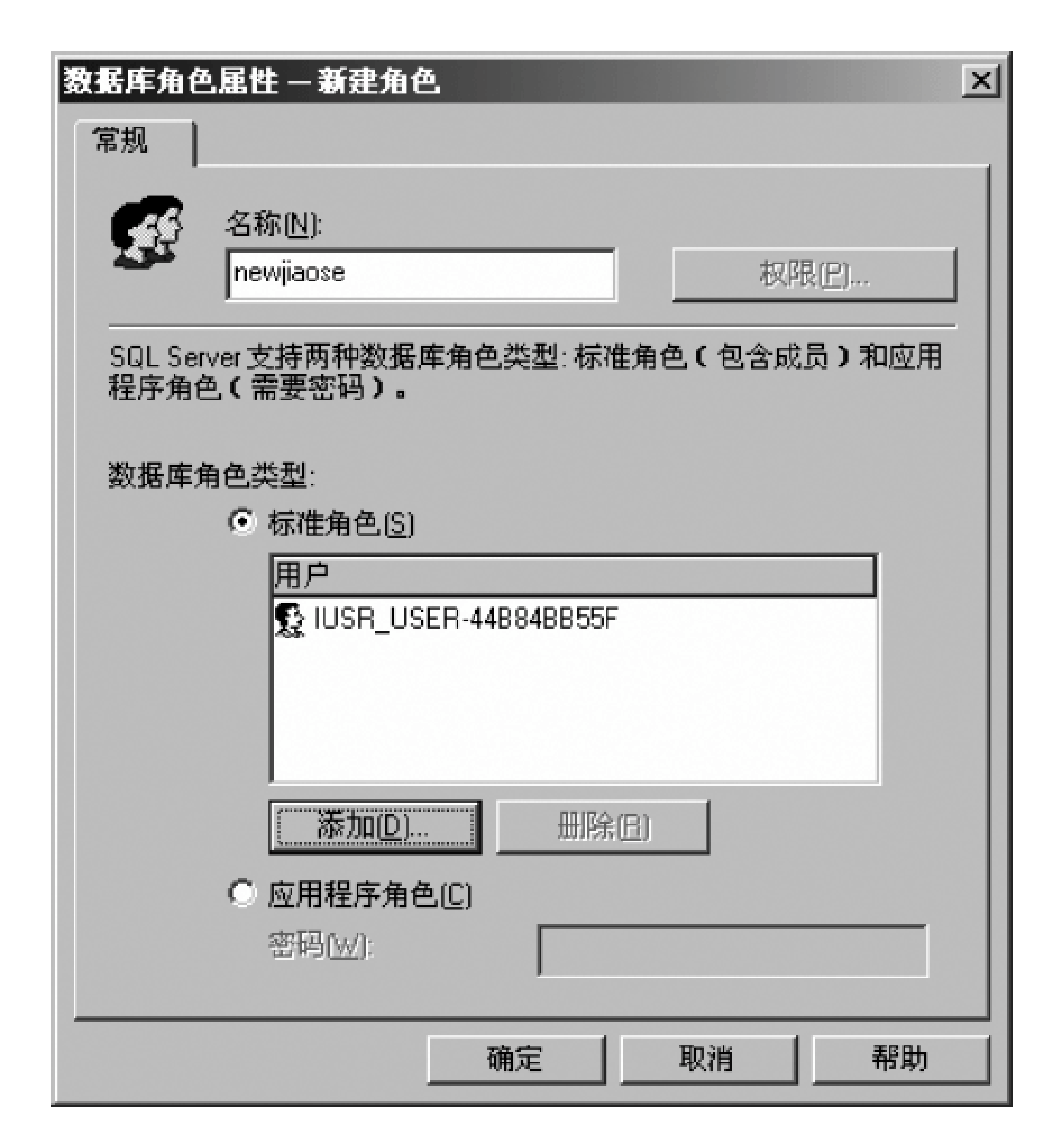


图 3-4-12　新建角色并添加角色的用户

(19) 重新打开 newjiaose 的属性,并单击"权限",在 mytable 一行将 SELECT、INSERT、UPDATE 和 DELETE 权限选中,并单击"确定",新建角色创建完成,如图 3-4-13 所示。

(20) 在 mydb 数据库文件夹的用户中打开 IUSR 的属性,选中 newjiaose,并确定,赋予 IUSR 用户以 newjiaose 权限,如图 3-4-14 所示。



图 3-4-13　设置角色访问 mytable 的权限



图 3-4-14　设置 IUSR 的数据库角色

(21) 修改 conn.asp 文件为以下内容。

```
<%
set Conn=Server.CreateObject("ADODB.Connection")
Conn.Open "provider=sqloledb;server=127.0.0.1;database=mydb;integrated security=sspi"
%>
```

(22) 重新打开默认主页，发现可以正确显示，使用 SQL 注入攻击添加账户，发现已经不能实现。

(23) 修改 SQL Server 内置存储过程。

SQL Server 内置了一批危险的存储过程。可以读到注册表信息、写入注册表信息、

执行命令和读磁盘共享信息等。

危险的内置存储过程有：

```
XP_cmdshell
xp_regaddmultistring
xp_regdeletekey
xp_regdeletevalue
xp_regenumkeys
xp_regenumvalues
xp_regread
xp_regremovemultistring
xp_regwriteActiveX 自动脚本：sp_OAcreate
sp_OADestroy
sp_OAMethod
sp_OAGetProperty
sp_OASetProperty
sp_OAGetErrorInfo
sp_OAStop
```

以上各项全在封杀之列，例如 xp_cmdshell 屏蔽的方法为：sp_dropextendedproc'xp_cmdshell'，如果需要的话，再用 sp_addextendedproc 'xp_cmdshell','xpsql70. dll'进行恢复。如果不知道 xp_cmdshell 使用的是哪个. dll 文件的话，可以使用 sp_helpextendedproc xp_cmdshell 来查看 xp_cmdshell 使用的是哪个动态连接库。另外，将 xp_cmdshell 屏蔽后，还需要做的步骤是将 xpsql70. dll 文件进行改名，以防止获得 sa 的攻击者将它进行恢复。

(24) 修改脚本防止 SQL 注入。

① 新建文件 noinject. asp，自定义两个 asp 函数 ReqNum 和 ReqStr 进行 url 输入过滤，防止 SQL 注入。

```
<%
Function ReqNum(StrName)
ReqNum=Request(StrName)
if Not isNumeric(ReqNum)then
Response.Write"参数必须为数字型!"
Response.End
End if
End Function

Function ReqStr(StrName)
ReqStr=Replace(Request(StrName),"'","''")
End Function
%>
```

② 将 showid. asp 文件作出如下修改以调用过滤函数。

文件 3：showid. asp

```
<!--#include file="conn.asp"-->
```

```
<!--#include file="noinject.asp"-->
<%
set rs=server.createobject("adodb.recordset")
sql="select * from mytable where id="& ReqNum("id")
rs.open sql,conn,1,1
%>
```

其后内容不变。

③ 再次进行注入攻击，结果如图 3-4-15 所示，可见注入攻击失败。

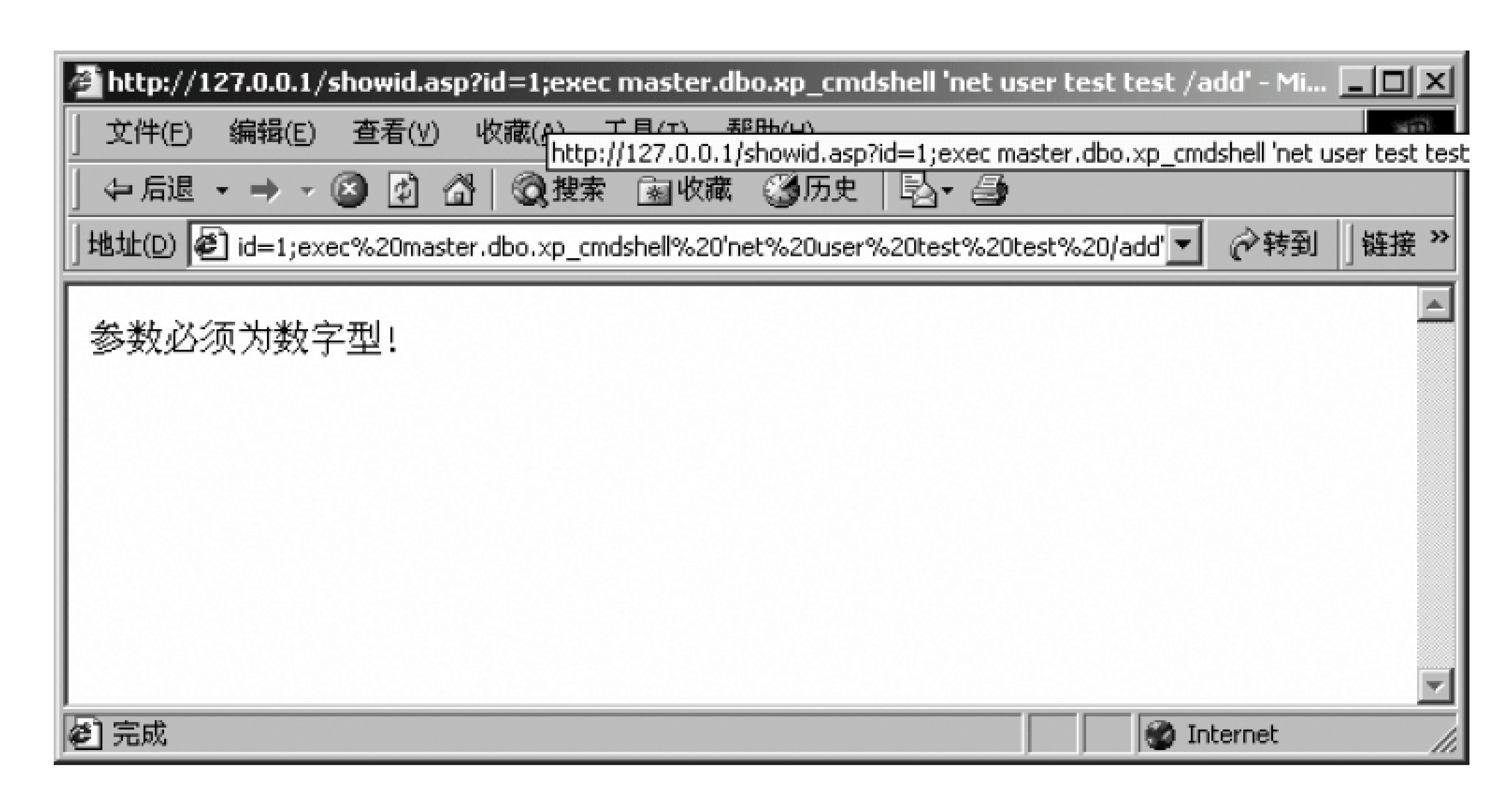


图 3-4-15　SQL 防注入效果

3.4.8　实验思考

数据库的安全性与操作系统的安全性有没有关系。

3.5　网络安全通信

3.5.1　实验类型

综合型，4 学时，必选实验。

3.5.2　实验目的

通信安全是网络安全的重要内容之一。通过实验，使学生认识安全通信的必要性，了解常用的安全协议，掌握常用的网络安全通信实现方法。

3.5.3　题目描述

使用 Windows 2000 Server 操作系统建立 VPN 和 IPSec 安全通信。

3.5.4 实验要求

能够在 Windows 2000 Server 上建立 VPN 服务器并正确设置其参数，建立 VPN 客户端连接到 VPN 服务器，实现远程访问局域网，能够使用 IPSec 实现安全通信。

3.5.5 相关知识

(1) 众所周知，Internet 充满着威胁，普通方式的邮件传递、浏览网页等都可能被嗅探工具捕获造成损失。使用虚拟专用网络(VPN)，移动职员和上班较远的人员可以通过 Internet 安全地访问他们公司的局域网(LAN)。按微软的定义，虚拟专用网(Virtual Private Network，VPN)涵盖了跨共享网络或公共网络的封装、加密和身份验证链接的专用网络的扩展。VPN 连接可以通过 Internet 提供远程访问和到专用网络的路由选择连接。

通过建立的 VPN 连接，使用自动安装在计算机上的点对点隧道协议(PPTP)或第二层隧道协议(L2TP)，就可以经由 Internet 或其他网络连接到 Windows 2000 远程访问服务器(即 VPN 服务器)来安全地访问网络资源。

图 3-5-1 所示为用户主机直接连接到 Internet，并通过 Internet 连接到远程访问服务器。为使 Internet 上的主机能够访问到 VPN 服务器(即远程访问服务器)，VPN 服务器必须拥有一个公有 IP 地址。VPN 服务器一般具有双网卡，分别连接到 Internet 和内部网络。

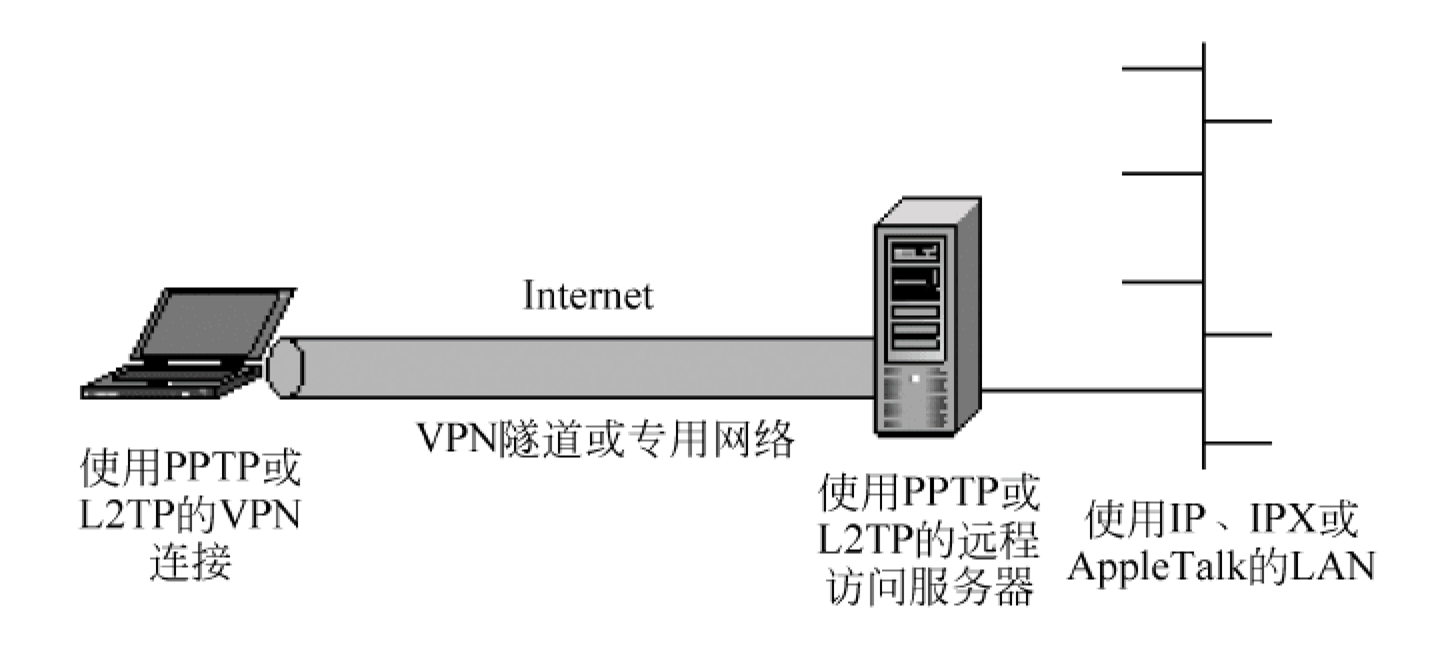


图 3-5-1　用户直接连接到 Internet 并建立 VPN 连接

使用 VPN 的优点如下。

① 降低费用：通过 Internet 访问比采用长途电话的方式更能节省费用。

② 较强的安全性：远程访问服务器强制执行身份验证和加密协议，通过 VPN 进行的 Internet 连接是加密的和安全的。

③ 网络协议支持：由于支持最常用的网络协议(包括 TCP/IP、IPX 和 NetBEUI)，因此可以远程运行任何依赖于这些特殊网络协议的应用程序。

④ IP 地址安全：因为 VPN 是加密的，所以远程访问服务器分配的 VPN 连接的内部

地址不能被 Internet 上的用户看到。Internet 上的用户仅能看到远程访问服务器的外部 IP 地址。

如果有 Winsock 代理客户在活动,则不能创建 VPN。因为还没等数据以 VPN 要求的方式被处理,Winsock 代理客户就已经将数据重定向到了已配置好的代理服务器上。因此要建立 VPN,首先应该禁用 Winsock 代理客户。

(2) IPSec 简介。

IPSec 实际上是一套协议包而不是单个的协议,IPSec 是在 IP 网络上保证安全通信的开放标准框架,它在 IP 层提供数据源验证、数据完整性和数据保密性。其中比较重要的有 RFC2409 IKE(Internet Key Exchange)互联网密钥交换、RFC2401 IPSec 协议、RFC2402 AH(Authentication Header)验证包头和 RFC2406 ESP(Encapsulating Security Payload)加密数据等协议。IPSec 独立于密码学算法,这使得不同的用户群可以选择不同的安全算法。

IPSec 主要由 AH(认证头)协议,ESP(封装安全载荷)协议以及负责密钥管理的 IKE(因特网密钥交换)协议组成。AH 为 IP 数据包提供无连接的数据完整性和数据源身份认证。数据完整性通过消息认证码(如 MD5、SHA1)产生的校验值来保证,数据源身份认证通过在待认证的数据中加入一个共享密钥来实现。ESP 为 IP 数据包提供数据的保密性(通过加密机制)、无连接的数据完整性、数据源身份认证以及防重防攻击保护。AH 和 ESP 可以单独使用,也可以配合使用,通过组合可以配置多种灵活的安全机制。密钥管理包括 IKE 协议和安全联盟 SA(Security Association)等部分。IKE 在通信双方之间建立安全联盟,提供密钥确定、密钥管理机制,是一个产生和交换密钥材料并协商 IPSec 参数的框架。IKE 将密钥协商的结果保留在 SA 中,供 AH 和 ESP 通信时使用。

IPSec 工作模式支持传输模式和隧道模式,在公共 IP 网上建立私有 IP 地址的 VPN 就只能使用隧道模式了。

3.5.6 实验设备

主流配置 PC 一台,Windows 2000 Server 操作系统,网络环境。

3.5.7 实验步骤

1. 建立实验环境

(1) 禁用实验主机防火墙。

(2) 实验主机 IP 配置。

在本实验中,实验主机配置了两个网卡,分别是“本地连接”和“本地连接 2”。现在分别对这两块网卡进行配置(在本实验中主机采用的是 Windows 7 系统,可能配置过程和显示界面与 XP 不同)。

① 对本地连接进行配置:右击“本地连接”,在“网络”选项卡中双击“Internet 协议版

本 4(TCP/IPv4)”,在弹出的对话框中将“IP 地址”设置为“192.168.1.10”将“子网掩码”设置为“255.255.255.0”,将“网关”设置为“192.168.1.254”,将“DNS 服务器”设置为“61.155.18.30”,如图 3-5-2 所示。

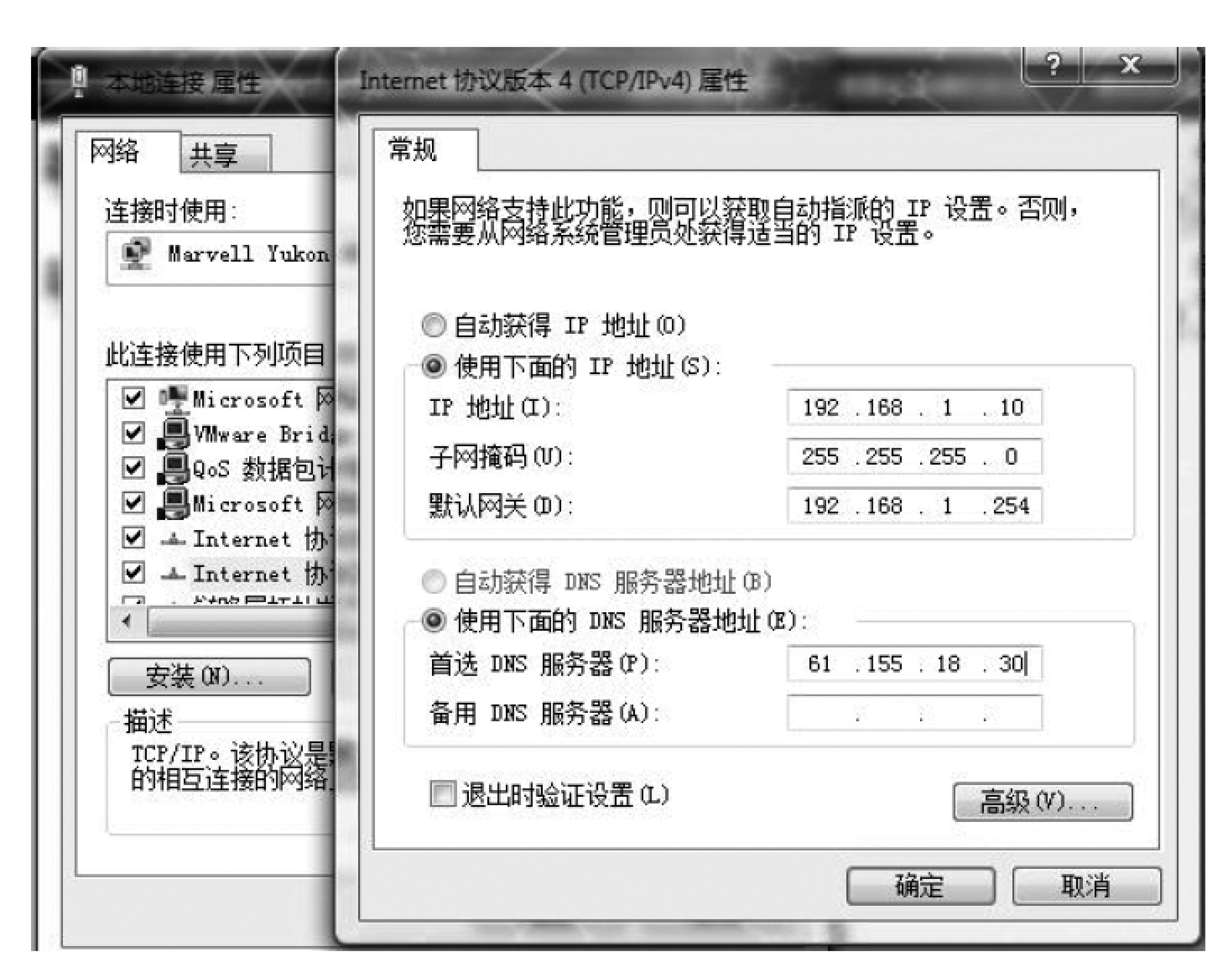


图 3-5-2　实验主机“本地连接”网卡(TCP/IPv4)属性配置

② 如果“本地连接 2”没有激活,则需要先激活该网络接口。

③ 对“本地连接 2”进行配置:右击“本地连接 2”,在“网络”选项卡中双击“Internet 协议版本 4(TCP/IPv4)”,在弹出的对话框中将“IP 地址”设置为“192.168.3.10”,将“子网掩码”设置为“255.255.255.0”,如图 3-5-3 所示。



图 3-5-3　实验主机“本地连接 2”网卡(TCP/IPv4)属性配置

（3）虚拟网络设置。

① 打开 VMware Workstation 软件，单击“编辑”菜单，在下拉列表中选择“虚拟网络编辑器”选项。

② 在弹出的对话框中单击“添加网络”按钮，选择 VMnet2，并将其桥接到主机网卡为本地连接的网络适配器（即 Marvell Yukon 88E8059 Family PCI-E Gigabit Ethernet Controller）。

③ 再按同样的方法添加 VMnet3 的网络，将其桥接到主机网卡为本地连接 2 的网络适配器，如图 3-5-4 所示。

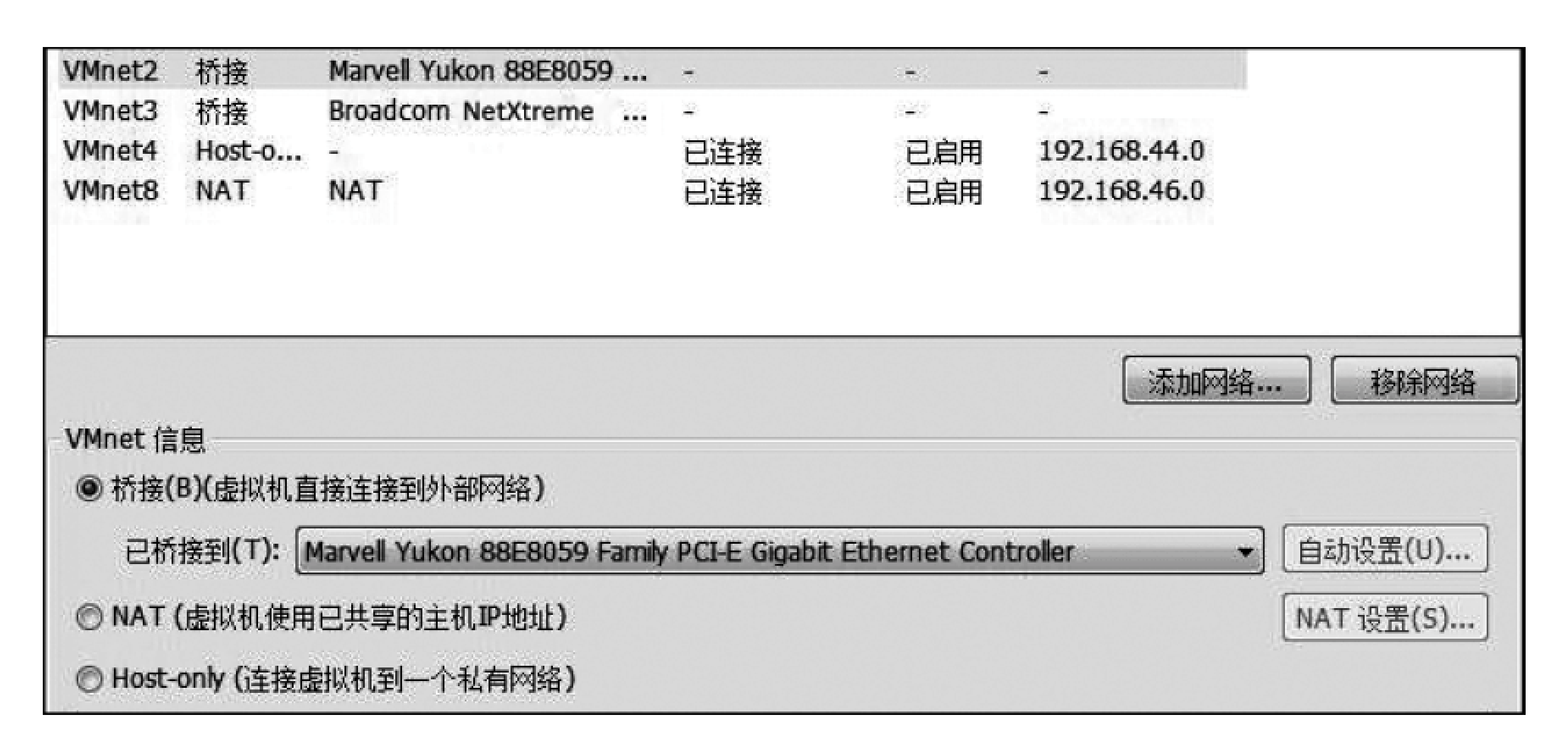


图 3-5-4 更改桥接模式

（4）虚拟机网配置。

① 启动虚拟机，在该选项卡中选择“编辑虚拟机设置”选项，如图 3-5-5 所示。



图 3-5-5 Windows Server 2003 的启动界面

② 在弹出的对话框中单击“添加”按钮，在“添加硬件向导”中选择“网络适配器”选项，单击“下一步”按钮，再单击“完成”按钮，如图 3-5-6 所示。



图 3-5-6 添加网络适配器

③ 将网络适配器的连接类型设置为“自定义”，选择 VMnet2 的桥接模式，如图 3-5-7 所示。同理，将网络适配器 2 的连接类型设置为“VMnet3(桥接)”，如图 3-5-8 所示。



图 3-5-7 更改网络适配器的连接模式

(5) 虚拟主机网卡 TCP/IP 属性的配置。

① 启动 Windows Server 2003 虚拟机。



图 3-5-8　更改网络适配器 2 的连接模式

② 对本地连接虚拟机网卡的 TCP/IP 属性进行设置，将“IP 地址”设置为“192.168.1.110”，将“子网掩码”设置为“255.255.255.0”将“网关”设置为“192.168.1.254”，如图 3-5-9所示。

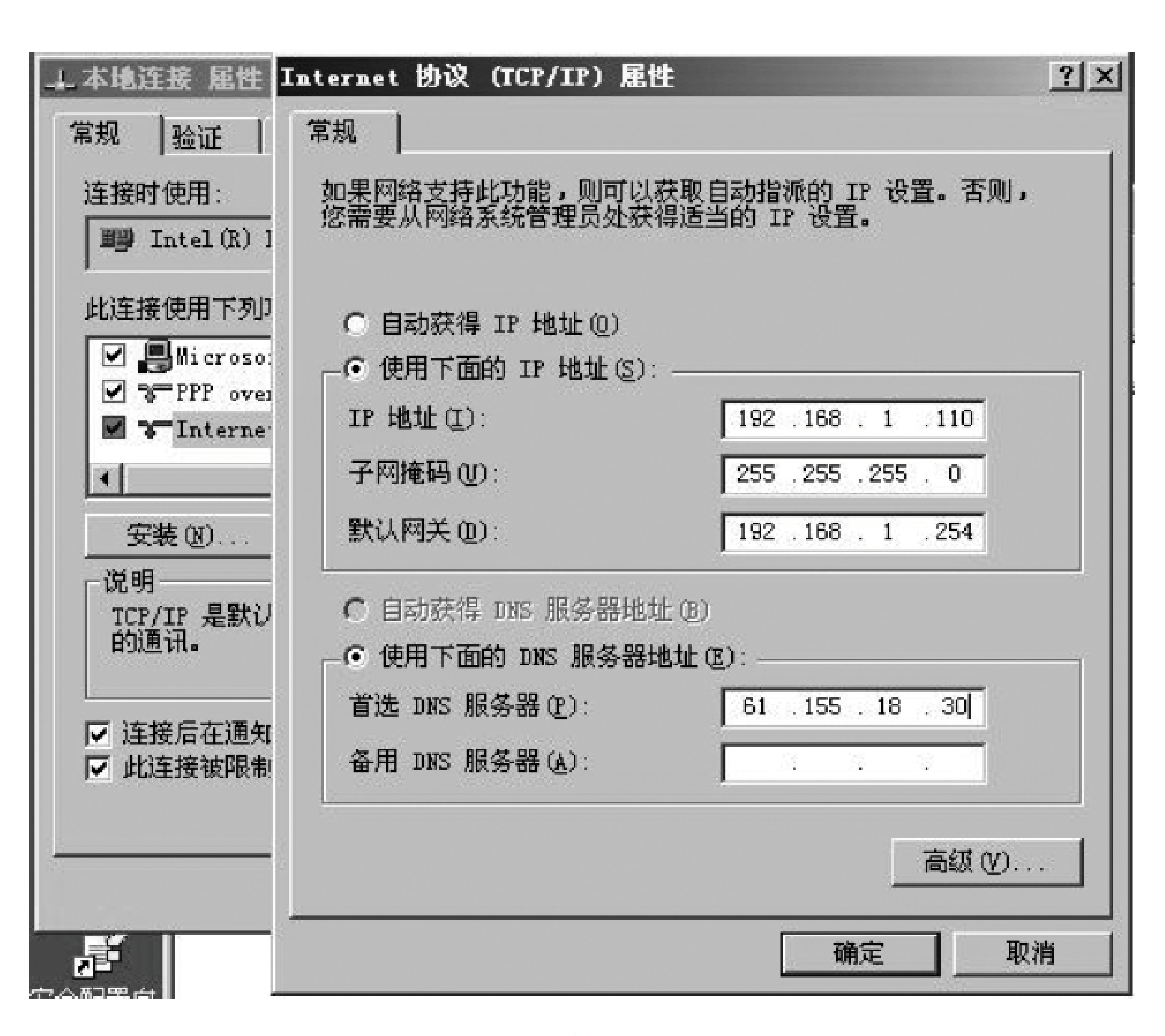


图 3-5-9　虚拟主机本地连接的网卡的 TCP/IP 属性配置

③ 对本地连接 2 进行配置：将“IP 地址”设置为“192.168.2.110”，将“子网掩码”设置为“255.255.255.0”，如图 3-5-10 所示。

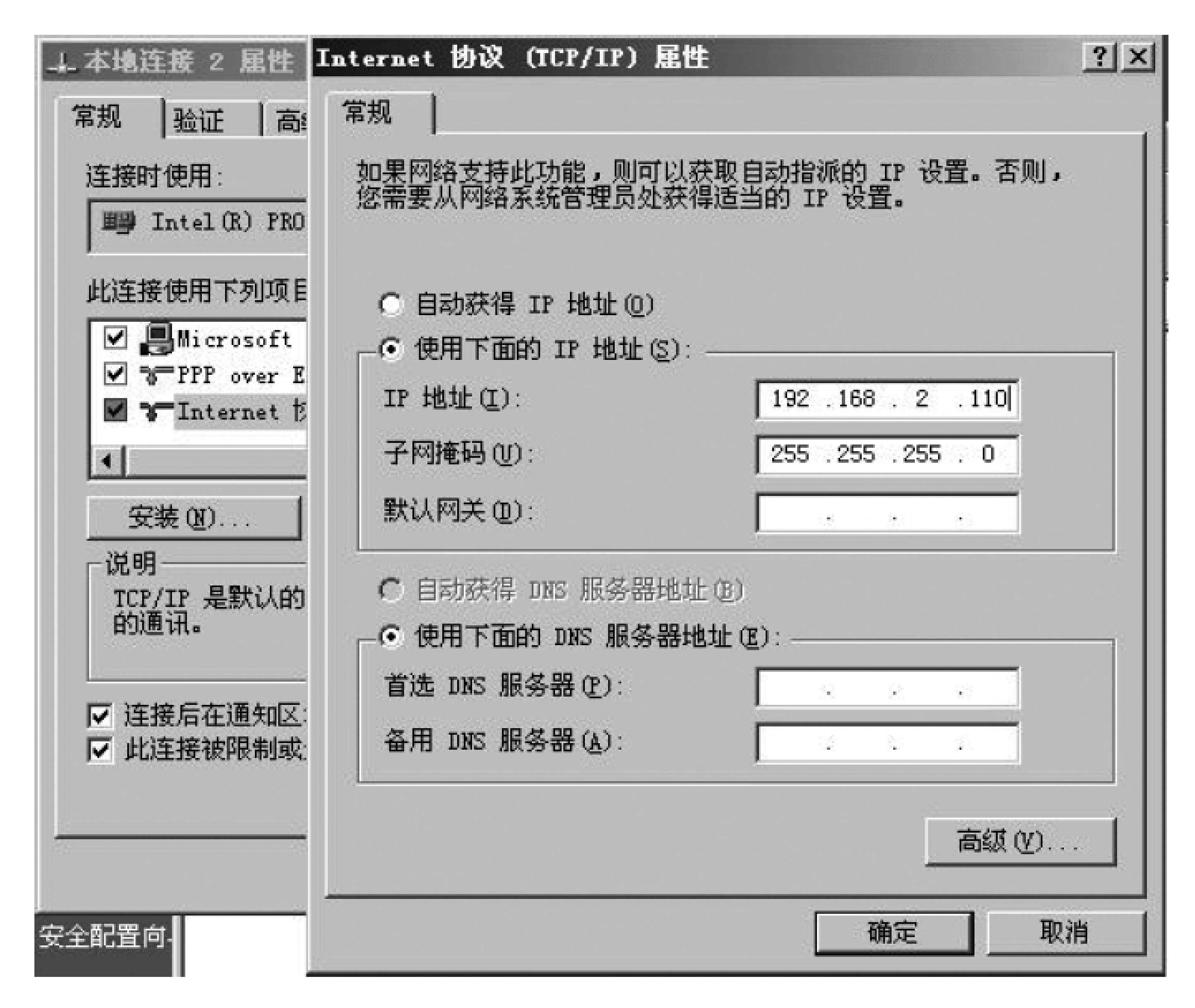


图 3-5-10　虚拟主机本地连接 2 的网卡的 TCP/IP 属性配置

2. 在 Windows 2003 Server 平台下构建 PPTP VPN 服务器

(1) 打开路由和远程访问。

在 Windows 2003 Server 虚拟服务器中依次选择“开始”→“程序”→“管理工具”→“路由和远程访问”，打开“路由和远程访问”的控制台，如图 3-5-11 所示。

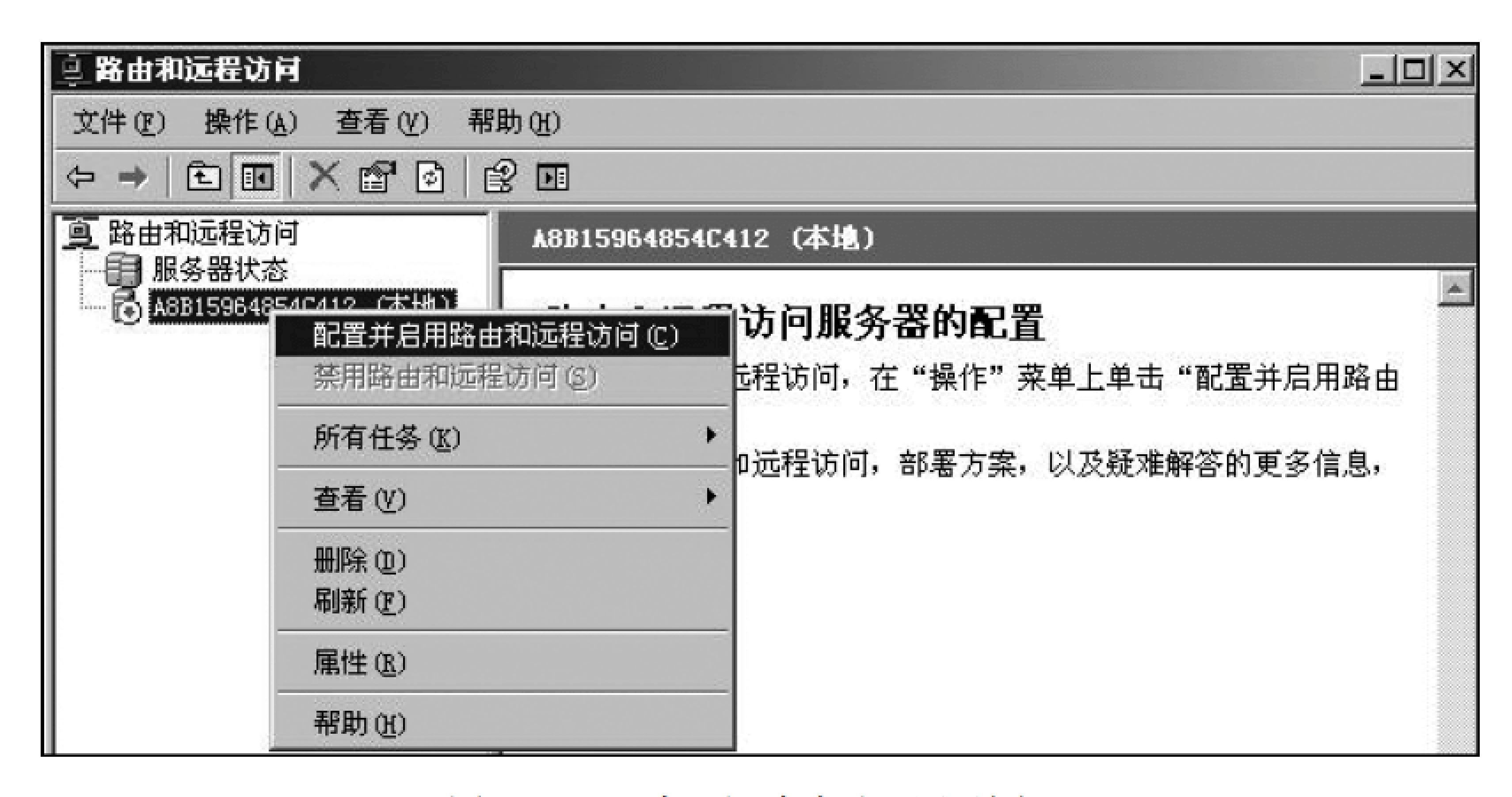


图 3-5-11　打开“路由和远程访问”

(2) 配置路由和远程访问服务器。

右击服务器名，选择“配置并启用路由和远程访问”选项，配置过程如图 3-5-12 至图 3-5-17所示。

最后单击“下一步”按钮，再单击“完成”按钮即可。

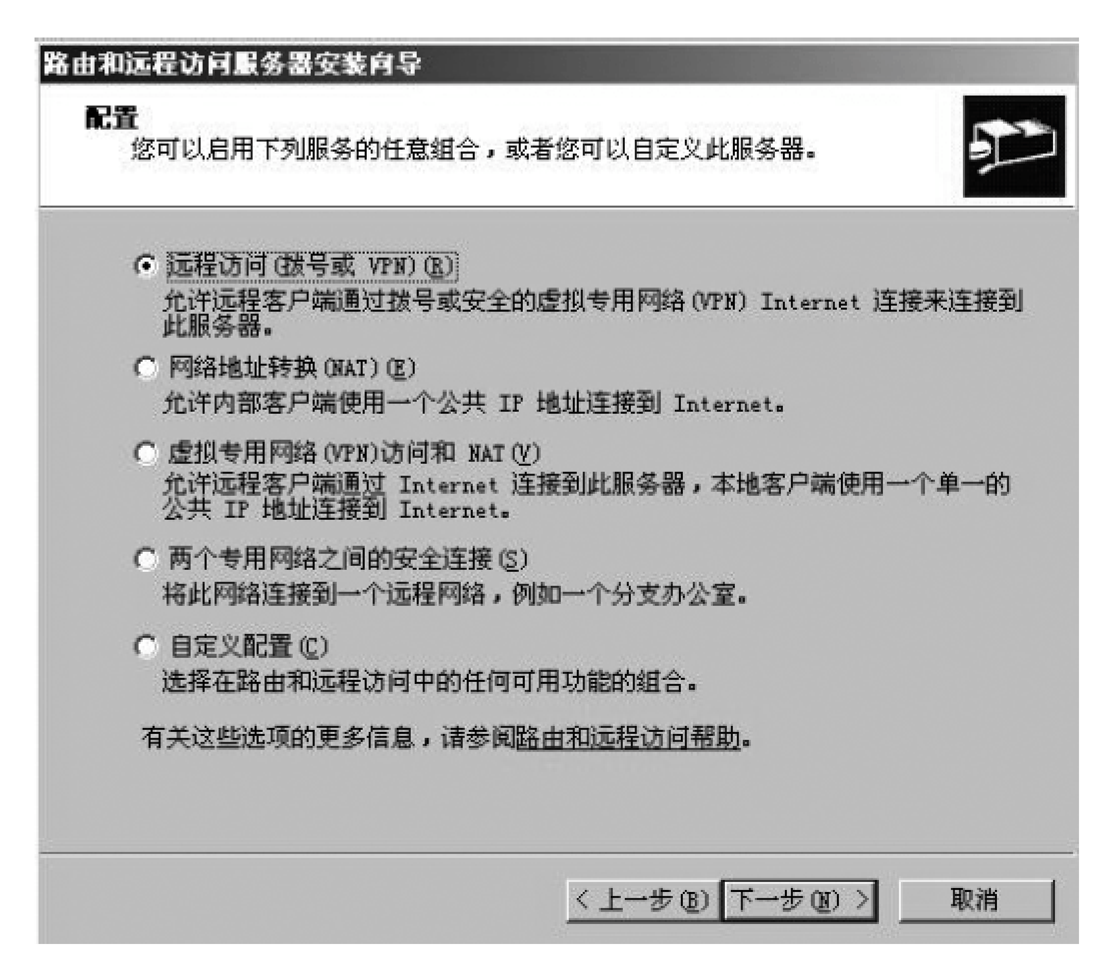


图 3-5-12 “配置”对话框

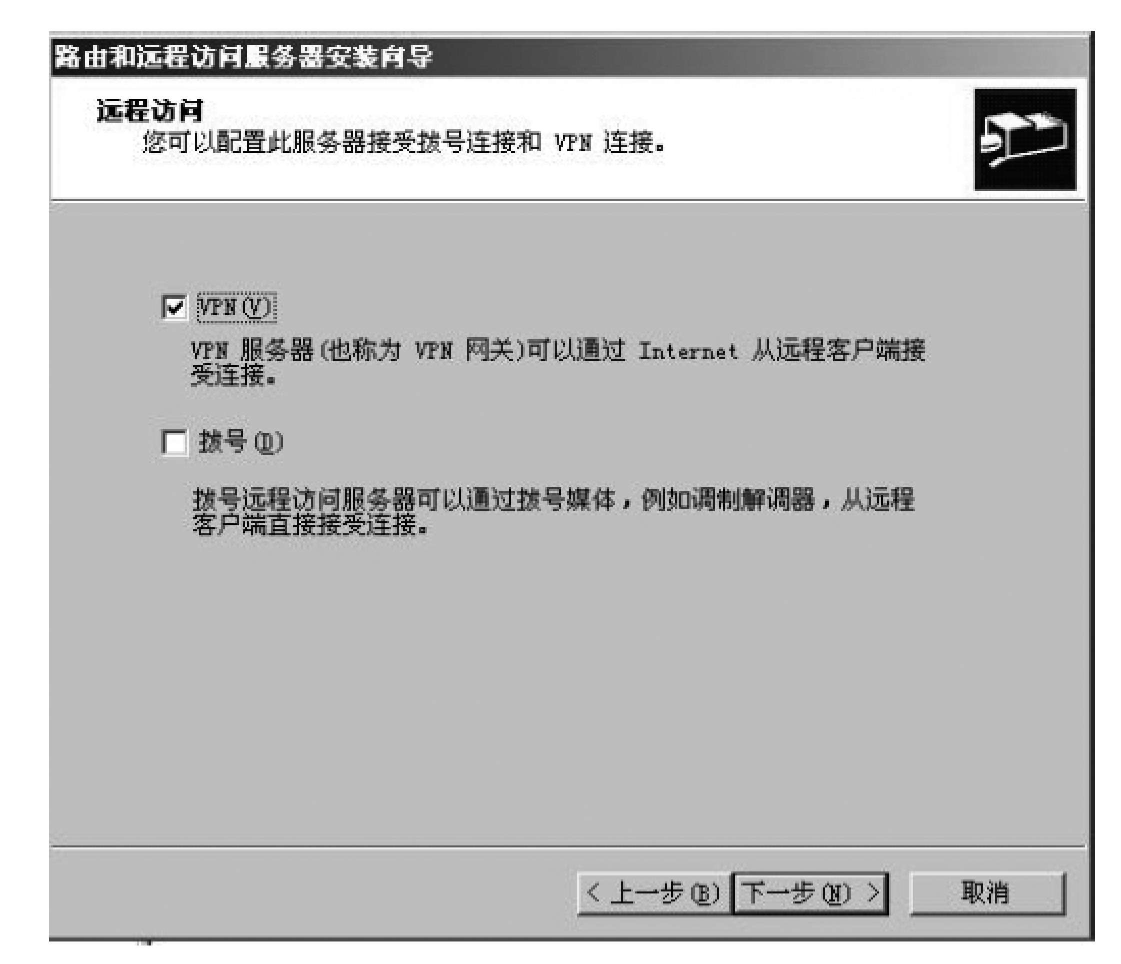


图 3-5-13 “远程访问”对话框

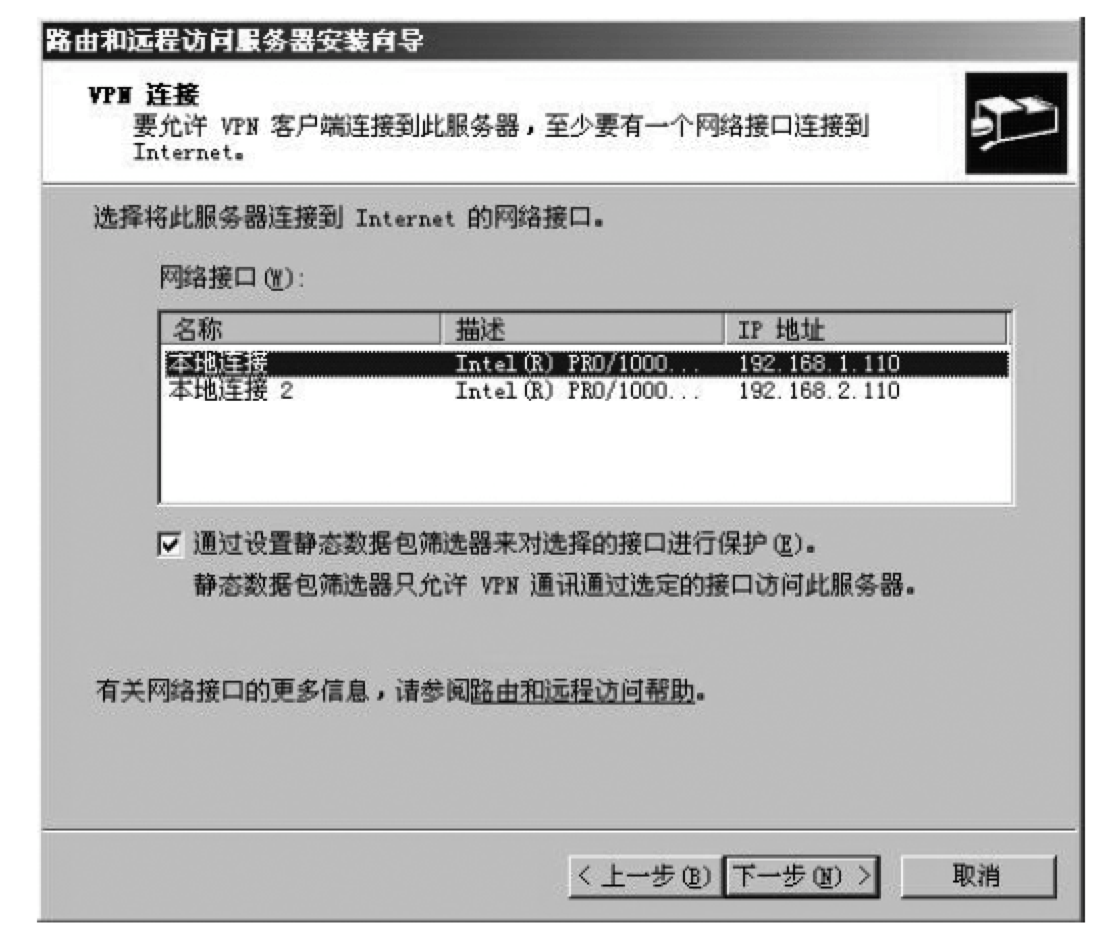


图 3-5-14 “VPN 连接”对话框

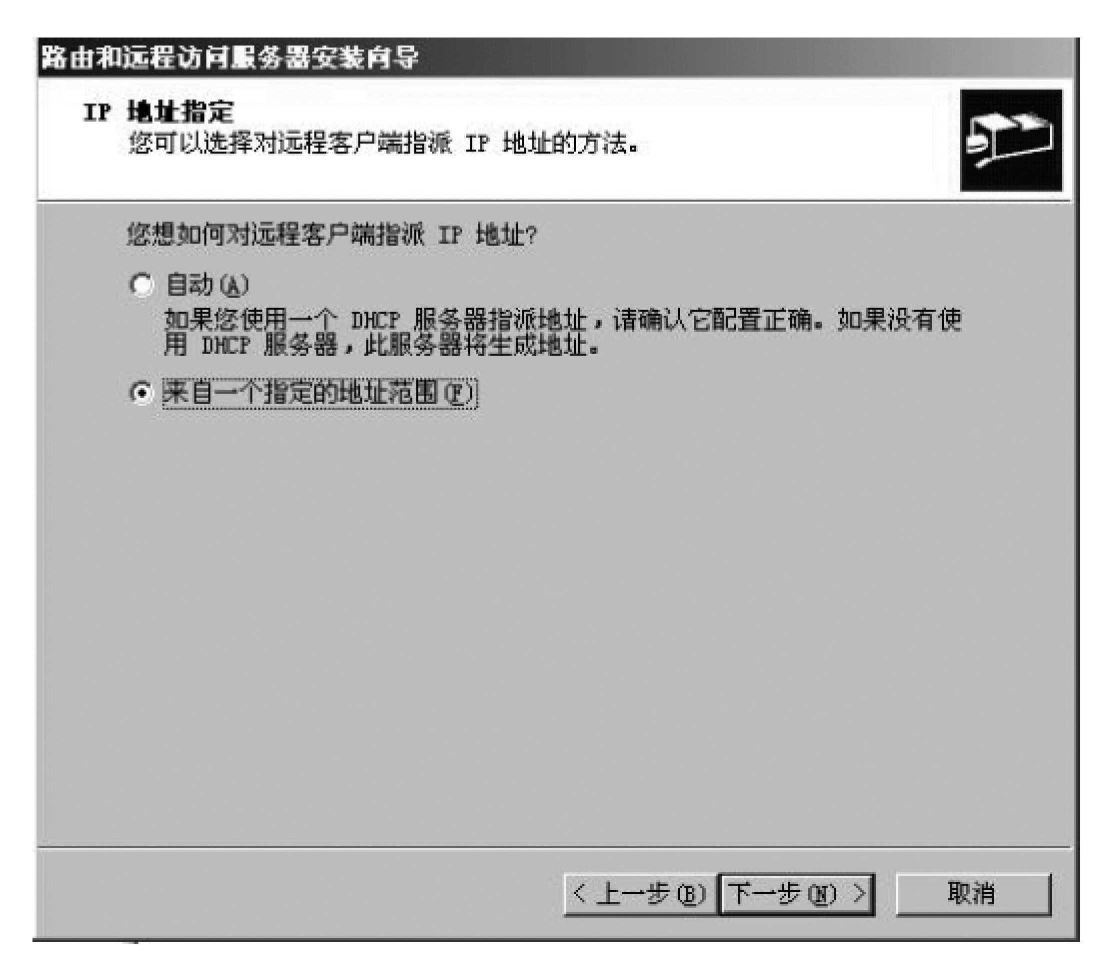


图 3-5-15 “IP 地址指定”对话框

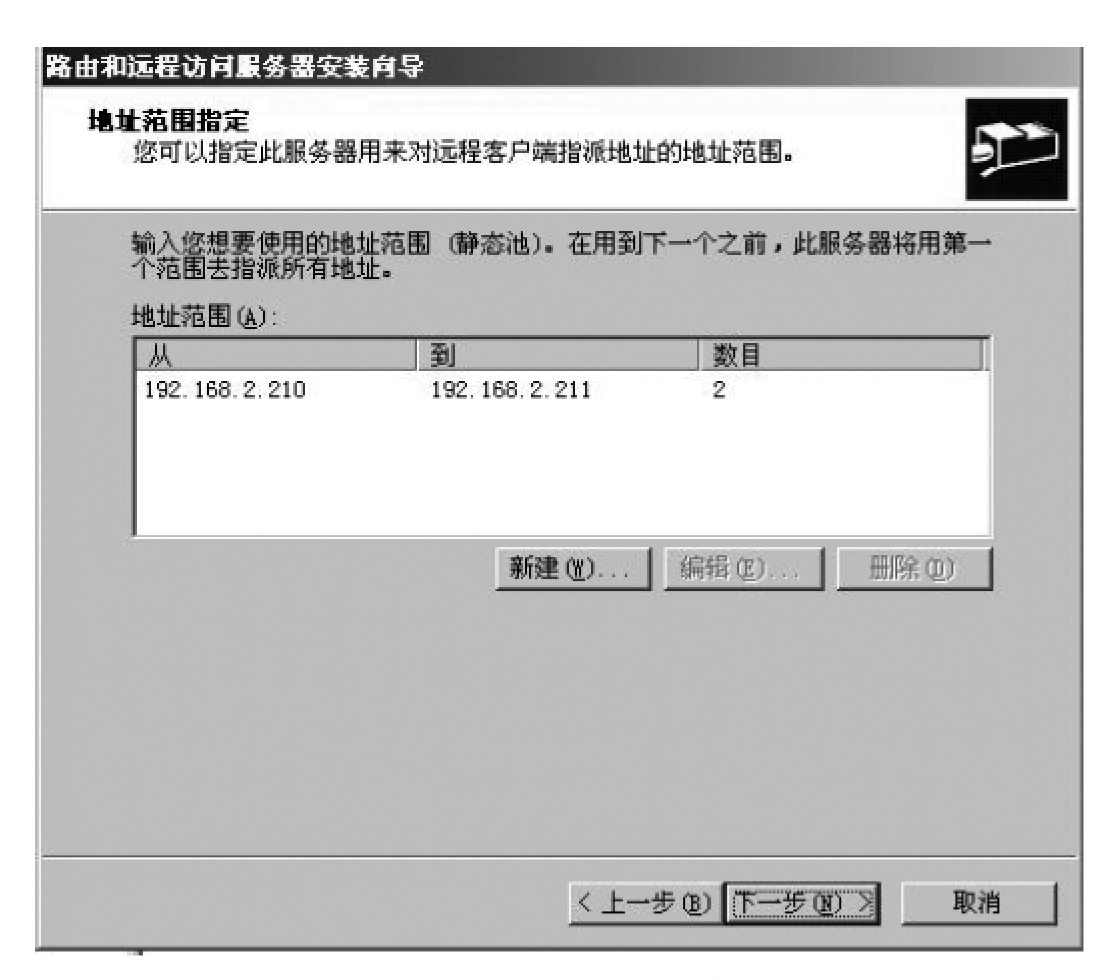


图 3-5-16 “地址范围指定”对话框

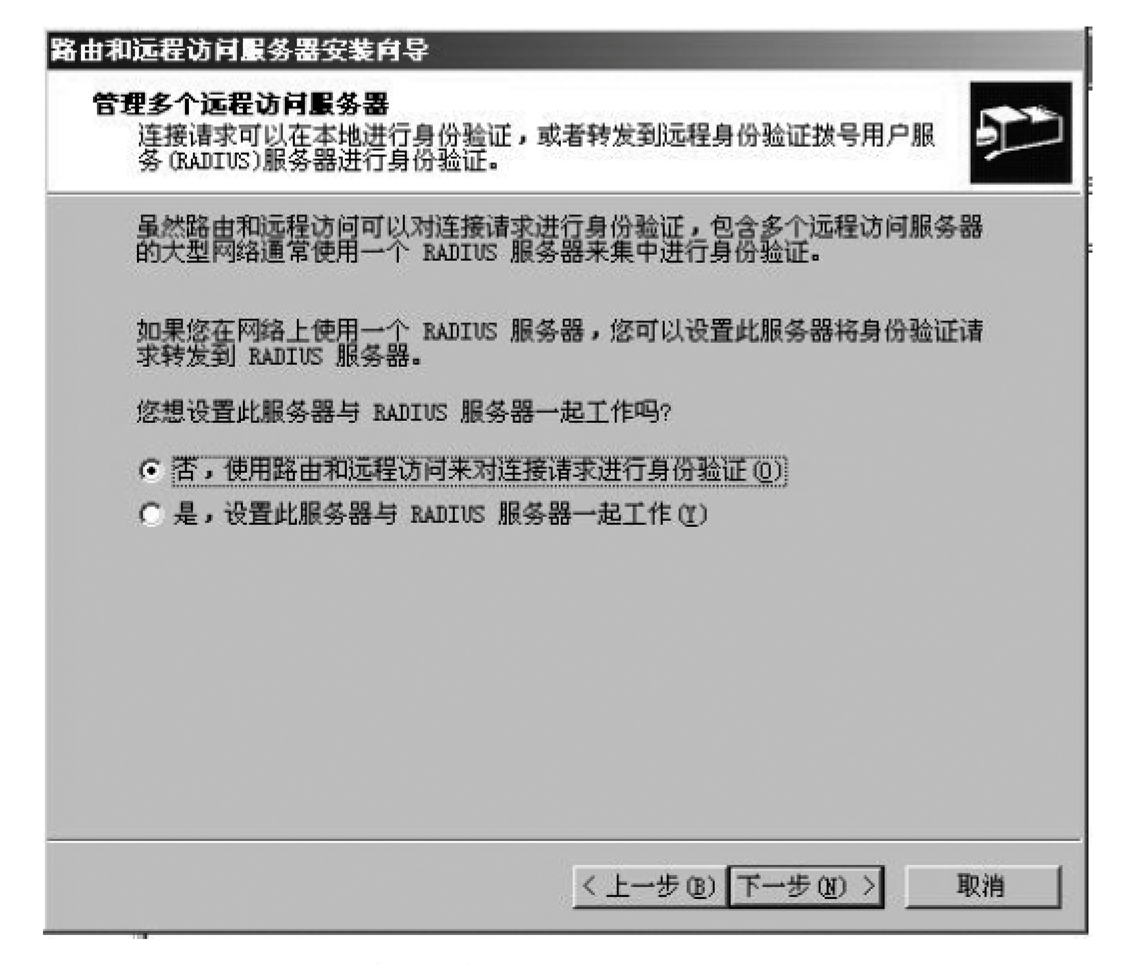


图 3-5-17 “管理多个远程访问服务器”对话框

3. 配置 Windows PPTP VPN 服务器

(1) 修改身份认证配置。

① 右击安装好的服务器名(因为之前的名字有点长,现在改为 NB74110),在“安全”标签中将“身份验证提供程序:”改为“Windows 身份验证”,如图 3-5-18 所示。

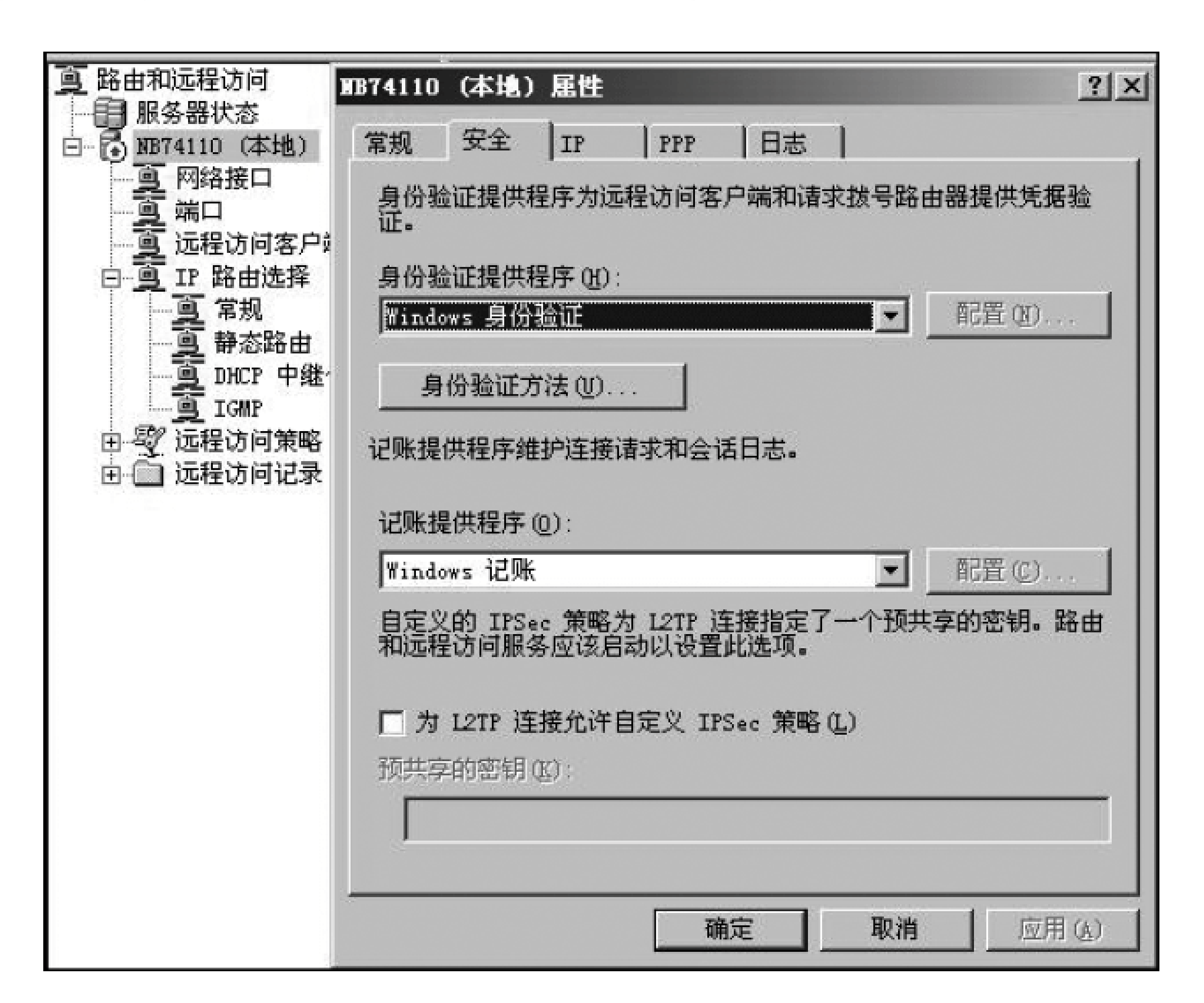


图 3-5-18 VPN 服务器身份验证方式配置

② 右击“端口”,选择“属性”选项,在“端口 属性”对话框中选择“WAN 微型端口(PPTP)”,如图 3-5-19 所示。

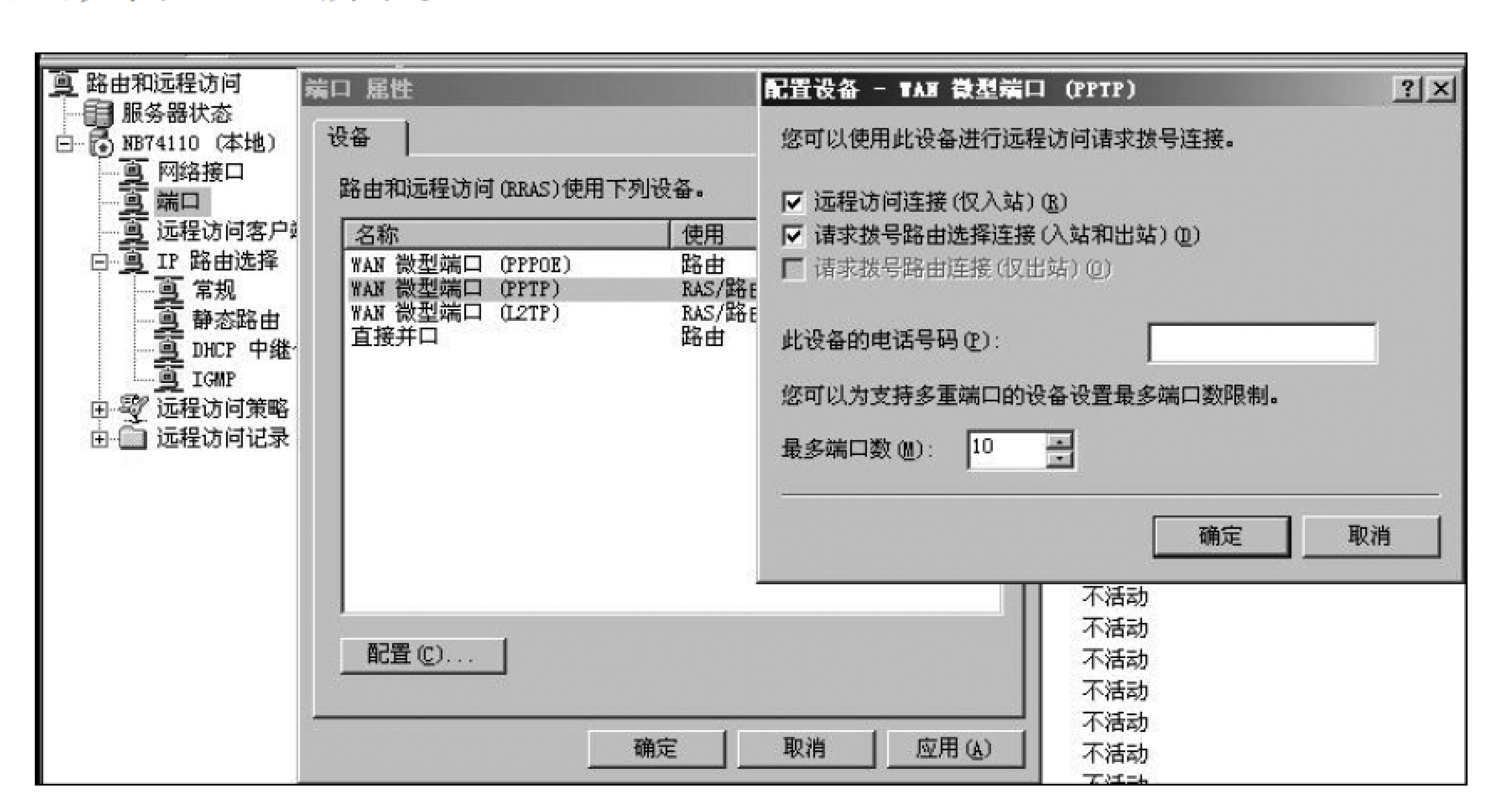


图 3-5-19 PPTP VPN 端口配置

(2) VPN 用户配置。

① 创建 VPN 用户。

右击“我的电脑”,依次选择“管理”→“本地用户和组”,右击“用户”,选择“新用户”选

项，在弹出的对话框中输入新建的用户名和密码(kings/abc)，最后单击“创建”按钮完成，如图 3-5-20 所示。



图 3-5-20　创建 VPN 用户

② 设置 VPN 用户访问权限。

右击 kings 用户，选择“拨入”标签页，将“远程访问权限(拨入或 VPN)”设为“允许访问”，如图 3-5-21 所示。



图 3-5-21　用户属性设置

③ 配置远程访问策略。

右击 VPN 服务器“远程访问策略”项中“到 Microsoft 路由选择和远程访问服务器的连接策略”，在弹出的属性对话框中选择“授予远程访问权限”单选项，然后单击“编辑配置文件”按钮，如图 3-5-22 所示。对客户端的 VPN 拨入连接时间、客户端的 IP 地址分配、客户端身份验证方式和 VPN 的加密通信方式分别进行如图 3-5-23 所示的配置。

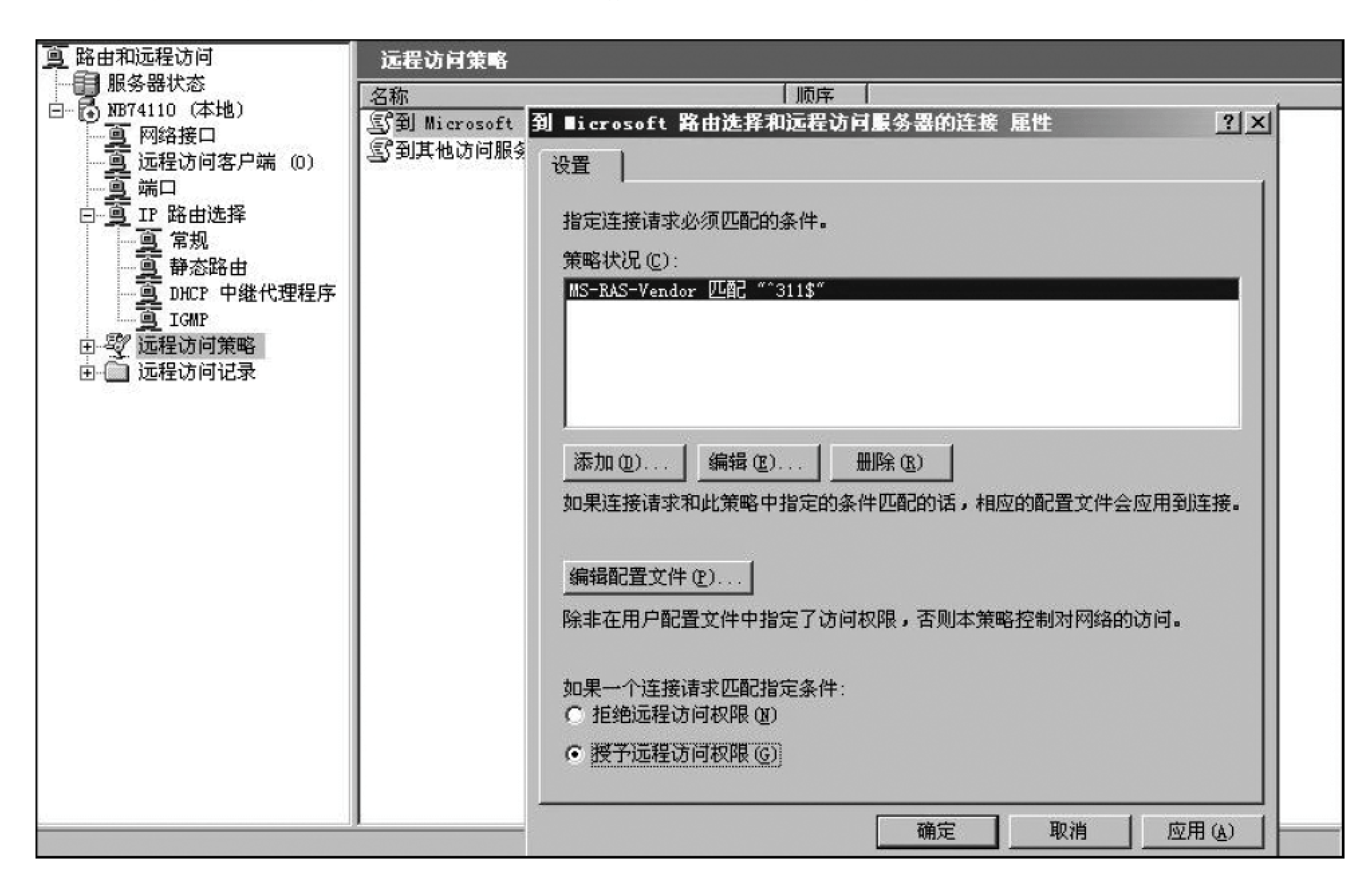


图 3-5-22　VPN 服务器远程访问策略属性配置



图 3-5-23　远程访问策略配置文件属性

4. 建立和配置 VPN 客户端

在主机的"控制面板"中依次选择"网络和 Internet"→"网络和共享中心",出现如图 3-5-24所示的对话框。



图 3-5-24 网络连接

单击"设置新的连接或网络",弹出如图 3-5-25 所示的对话框,选择"连接到工作区"。



图 3-5-25 选择连接选项

在“连接到工作区”对话框中选择“使用我的 Internet 连接(VPN)”,如图 3-5-26 所示。



图 3-5-26 连接到工作区的连接

单击“下一步”按钮,弹出如图 3-5-27 所示的对话框,输入 Internet 地址和目标名称,然后单击“下一步”按钮,单击“完成”按钮,即完成 VPN 客户端的建立。



图 3-5-27 输入要连接的 Internet 地址

5. VPN 运用和测试

（1）打开“控制面板”，选择“网络和 Internet”→“网络连接”，双击新建立的 PPPTP-VPN-SERVER 客户端，如图 3-5-28 所示。



图 3-5-28　打开网络连接

打开如图 3-5-29 所示的客户端，输入 VPN 用户名、密码信息。单击“连接”按钮。如果输入的用户名、密码是“身份验证配置”中设置的用户名、密码（kings/abc），那么 Windows 7 客户将成功连上，如图 3-5-30 所示。



图 3-5-29　连接 VPN 客户端



图 3-5-30　网络连接状态

单击“连接”按钮后，在无误的情况下，单击桌面右下角的网络连接后，显示 PPPTP-VPN-SERVER 已连接。

当客户端成功连接上时，在命令提示符环境下查看成功连接后的网络配置，如图 3-5-31 所示。

（2）Ping 测试。在 VPN 客户端上命令提示符环境中通过 Ping 命令测试内网，例如 Ping 192.168.2.110，如图 3-5-32 所示。

```
管理员: C:\windows\system32\cmd.exe
PPP 适配器 PPPTP-VPN-SERVER:

   连接特定的 DNS 后缀 . . . . . . . :
   IPv4 地址 . . . . . . . . . . . . : 192.168.2.211
   子网掩码  . . . . . . . . . . . . : 255.255.255.255
   默认网关. . . . . . . . . . . . . : 0.0.0.0

无线局域网适配器 无线网络连接 2:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 无线网络连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::dce5:4b7e:e998:1ec1%13
   IPv4 地址 . . . . . . . . . . . . : 192.168.1.10
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.1.254

以太网适配器 VMware Network Adapter VMnet1:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::f9db:7620:c4d6:30b8%22
   IPv4 地址 . . . . . . . . . . . . : 192.168.80.1
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :

以太网适配器 VMware Network Adapter VMnet8:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::9c6b:9f04:b3a:6b50%23
   IPv4 地址 . . . . . . . . . . . . : 192.168.46.1
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
```

图 3-5-31　VPN 客户端创建的 PPP 隧道连接

```
C:\Users\Administrator>ping 192.168.2.110

正在 Ping 192.168.2.110 具有 32 字节的数据:
来自 192.168.2.110 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.2.110 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.2.110 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.2.110 的回复: 字节=32 时间<1ms TTL=128

192.168.2.110 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

图 3-5-32　Ping 内网

3.5.8　实验思考

怎样证明采用以上措施的网络通信是安全的?

3.6　数字证书服务及加密认证

3.6.1　实验类型

综合型,8 学时,必选实验。

3.6.2 实验目的

数字证书主要应用于各种需要身份认证的场合，如网上银行、网上交易等，还可以应用于发送安全电子邮件、加密文件等方面。通过实验，使学生了解 PKI 的体系结构、证书机构（CA）的安装和配置，通过证书机构（CA）管理证书的方法，掌握数字证书的申请与安装，数字证书在网站、电子邮件的加密与认证等方面的应用。

3.6.3 题目描述

使用 Windows 2000 Server 建立数字证书颁发机构（CA），处理并颁发客户证书和服务器证书；在浏览器和 Web 服务器之间通过数字证书实现身份识别与加密通信；使用 RedHat Linux 9 操作系统架设邮件服务器，用户之间通过电子邮件数字证书实现身份识别。

3.6.4 实验要求

理解数字证书的原理和作用，能够建立 CA 并进行数字证书的颁发，能够申请、安装、使用 Web 服务器证书和客户证书，能够申请、安装、使用电子邮件证书。

提高要求：能够架设邮件服务器。

3.6.5 相关知识

随着 Internet 的分布越来越广泛，安全问题也日益突出，保护传送数据的需求也越来越强烈。在今天的 Internet 上，最常见的安全是通过使用数字证书实现的。数字证书可以在一个不信任的网络上辨识一个客户和服务器，并且可以加密数据。

目前，随着计算机技术、网络技术的发展，社会生活中传统的犯罪和不道德行为更加隐蔽和难以控制。人们从面对面的交易和作业，变成网上互相不见面的操作，没有国界、没有时间限制，可以利用互联网的资源和工具进行访问、攻击甚至破坏。

1. 安全认证中心（CA）、数字证书简介

数字证书是网络通信中标志通信各方身份信息的一系列数据，提供了一种在 Internet 上验证身份的方式，是由一个权威机构——CA 机构，又称为证书授权（Certificate Authority）中心发行的。数字证书是一个经证书授权中心数字签名的包含客户的公钥等与客户身份相关的信息，如客户唯一可识别名等。同时，CA 也可以提供时间戳、密钥管理及证书作废表（CRL）等服务。作为安全网络的公证机构，为了维护网络用户间的安全通信，CA 必须行使以下职能。

（1）管理和维护客户的证书和 CRL；

(2) 维护自身的安全;

(3) 提供安全审计的依据。

在基于证书的安全通信中,证书是证明用户合法身份和提供用户合法公钥的凭证,是建立保密通信的基础。因此,作为网络可信机构的证书管理设施,CA 的主要职能就是管理和维护它所签发的证书,提供各种证书服务,包括证书的签发、更新、回收、归档等。在各类证书服务中,除了证书的签发过程需要人为参与控制外,其他服务都可以利用通信信道通过用户与 CA 交换证书服务消息进行。CA 系统的主要功能是管理其辖域内的用户证书,因此,CA 系统功能及 CA 证书的应用紧紧围绕证书的管理而展开。

一个标准的 X.509 数字证书包含以下一些内容:

(1) 证书的版本信息;

(2) 证书的序列号,每个证书都有一个唯一的证书序列号;

(3) 证书所使用的签名算法;

(4) 证书的发行机构名称,命名规则一般采用 X.500 格式;

(5) 证书的有效期,现在通用的证书一般采用 UTC 时间格式,它的计时范围为 1950～2049;

(6) 证书所有人的名称,命名规则一般采用 X.500 格式;

(7) 证书所有人的公开密钥;

(8) 证书发行者对证书的签名。

2. 数字证书的用途

数字证书可以应用于公众网络上的商务活动和行政作业活动,包括支付型和非支付型电子商务活动,其应用范围涉及需要身份认证及数据安全的各个行业,包括传统的商业、制造业、流通业的网上交易,以及公共事业、金融服务业、工商税务海关、出入境检验检疫、政府行政办公、教育科研单位、保险、医疗等网上作业系统。

Internet 电子商务系统技术使在网上交易各方能够极其方便、轻松地获得政府、机构、商家和企业的信息,但同时也增加了某些敏感或有价值的数据被滥用的风险。交易各方在网上的一切行为都必须是真实可靠的,并且要使顾客、商家、企业和机构等交易各方都具有绝对的信心,因而因特网(Internet)电子商务系统必须保证具有十分可靠的安全保密技术,也就是说,必须依靠数字证书保证网络安全的四大要素,即信息传输的保密性、数据交换的完整性、发送信息的不可否认性和交易者身份的确定性。

数字证书采用公钥体制,即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥(私钥),用它进行解密和签名;同时设定一把公共密钥(公钥)并由本人公开,为一组用户所共享,用于加密和验证签名。当发送一份保密文件时,发送方使用接收方的公钥对数据加密,而接收方则使用自己的私钥解密,这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程,即只有用私有密钥才能解密。在公开密钥密码体制中,常用的一种是 RSA 体制。其数学原理是将一个大数分解成两个质数的乘积,加密和解密用的是两个不同的密钥。即使已知明文、密文和加密密钥(公开密钥),想要推导出解密密钥(私密密钥),在计算上是不可

能的。按现在的计算机技术水平,要破解目前采用的1024RSA密钥,需要上千年的计算时间。公开密钥技术解决了密钥发布的管理问题,商户可以公开其公开密钥,而保留其私有密钥。购物者可以用人人皆知的公开密钥对发送的信息进行加密,安全地传送给商户,然后由商户用自己的私有密钥进行解密。

3.6.6 实验设备

主流配置PC,Windows 2000 Server操作系统,IIS服务器,RedHat Linux 9操作系统,Foxmail电子邮件客户端,网络环境。

3.6.7 实验步骤

实验内容一:用SSL和数字证书实现安全Web访问

1. 建立认证中心(CA)

环境要求:Web服务器以Windows 2000 Server作为操作系统,认证中心与Web服务器位于同一主机,IP地址设为10.0.0.1,子网掩码设为255.255.255.0,浏览器为IE 4.0以上。

建立认证中心的过程是这样的:选择"控制面板"→"添加/删除程序"→"添加/删除Windows组件",在可选项中选择"证书服务",单击"详细信息",确保"证书服务Web注册支持"和"证书服务颁发机构(CA)"两个选项都被选中(如图3-6-1所示),开始安装。此时,系统会提示您一旦选择了证书服务,计算机的域和机器名是不可更改的。选择证书颁发的类型主要包括企业根CA、企业从属CA、独立根CA和独立从属CA。由于证书颁发机构的设置是很重要的,这里需要特殊说明,企业根CA和独立根CA都是证书颁发体系中最受信任的证书颁发机构,可以独立地颁发证书。企业根CA需要Active Directory支持,而独立根CA不需要。从属级的CA由于只能从另一证书颁发机构获取证书,所以一般不被选择。独立根CA可以选择在收到申请时自动颁发证书或将申请保持为搁置状态,由管理员验证证书申请者的真实性及合法性,决定是否颁发证书。可以根据需求选择

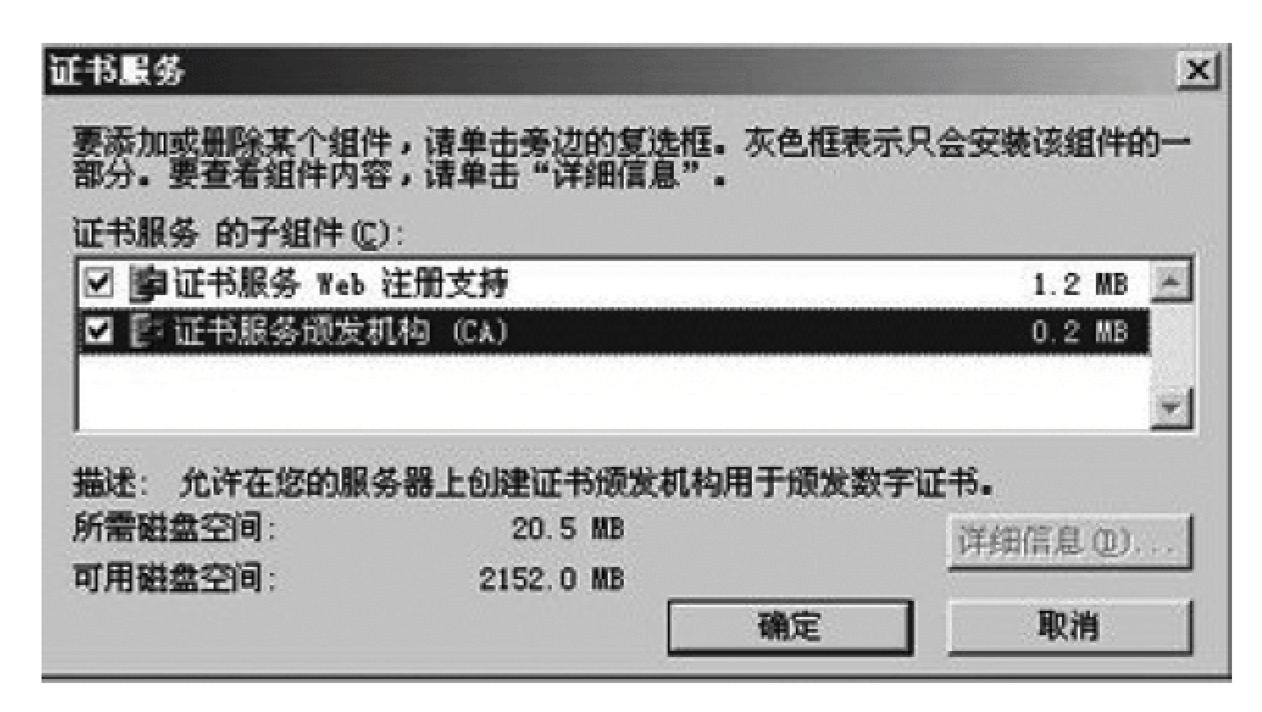


图3-6-1 "证书服务"对话框

合适的证书颁发类型。选好类型后，选择该页中的“高级”选项，进入下一步安装，填写 CA 的相关信息，如 CA 名称、单位、城市、电子邮件和有效期限等，再下一步进入高级选项页(如图 3-6-2 所示)，此时可以选择用来生成密钥对的加密服务提供程序(CSP)、散列算法和密钥长度，并选择现有的密钥及相关证书等。选项的选择取决于对安全程度的要求、计算机的复杂运算能力、对响应时间的要求和系统管理证书的负载程度等。单击“下一步”按钮，选择证书数据库及日志的位置，确认后即可进行安装。



图 3-6-2 “公钥/私钥对”对话框

设置证书服务管理：安装结束后，进行证书服务管理，如图 3-6-3 所示。对于独立根 CA 可以选择“在收到证书申请时确定证书颁发机构”的默认动作，设置方法是：打开“证书颁发机构”，单击 CA 名称，选择“属性”→“策略模块”→“配置”，选择“证书申请设为待定，系统管理员必须专门颁发证书”，这样管理者可以直接控制证书的发放。对于相关的申请，在“证书颁发机构”→“待定申请”中选择相应的申请证书，可以选择“颁发”或“拒绝”选项。在“已颁发证书”选项中选择相应证书，右击进行“吊销证书”的操作。



图 3-6-3 证书颁发机构窗口

2. 生成申请 Web 站点数字证书的文件

本操作在 Web 服务器端进行,具体步骤如下。

(1) 启动 Web 服务器的“Internet 信息服务”。

(2) 在“Internet 信息服务”中右击 MyWeb 站点名,选择快捷菜单的“属性”命令,出现“MyWeb 属性”对话框。

(3) 单击“MyWeb 属性”对话框中“目录安全性”页标签,再单击“服务器证书”按钮。

(4) 在“IIS 证书向导”对话框中,按提示,依次选择“创建一个新证书”→“现在准备请求,但稍候发送”等,设置有关属性,将最后的证书申请以文本文件保存,假设文件名为“C:\\certreq.txt”。

(5) 最后单击“完成”按钮即可。

3. 生成服务器证书

在 Web 服务器端依次执行如下步骤。

(1) 将证书申请文件内容复制到剪切板。方法是用记事本打开“C:\\certreq.txt”,查看申请文件内容。可以看到这是一个纯文本文件,以 PKCS#10 编码格式保存,首尾两行为申请的开始与结束。选择“编辑/全选”,再选择“编辑/复制”即可。

(2) 启动 IE,在地址栏输入“http://10.0.0.1/certsrv;”。

(3) 选择“申请证书”,单击“下一步”按钮。

(4) 选择申请类型为“高级申请”,单击“下一步”按钮。

(5) 选择第 2 项“使用 Base64 编码的 PKCS#10 文件提交一个证书申请,或使用 Base64 编码的 PKCS#7 文件更新证书申请”,单击“下一步”按钮。

(6) 右击中间“Base64 编码证书申请”右边的编辑框,选择快捷菜单选项“粘贴”,将证书申请内容粘贴进去。

(7) 单击“提交”按钮,完成申请功能。

(8) 打开证书服务器的“证书颁发机构”→“待定申请”,右击申请,选择“颁发”。

(9) 在 Web 服务器启动 IE,在地址栏输入“http://10.0.0.1/certsrv”,选择“检索 CA 证书或证书吊销列表”等提示,如图 3-6-4 所示,单击“下一步”按钮。

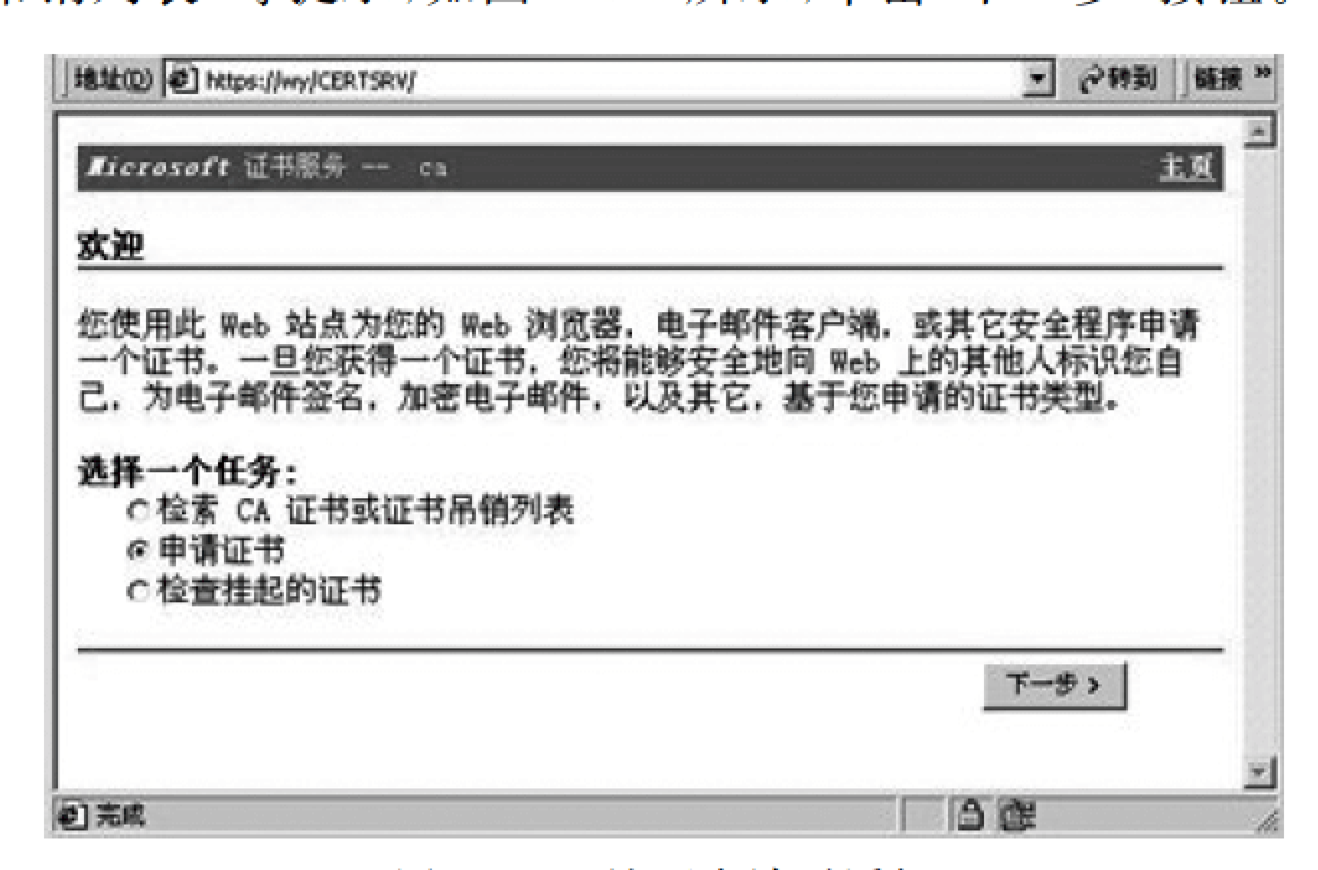


图 3-6-4 认证申请对话框

（10）选择“Base64 编码”，单击“下载 CA 证书”，如图 3-6-5 所示，将证书以 mywebcert.cer 为文件名保存在桌面上。

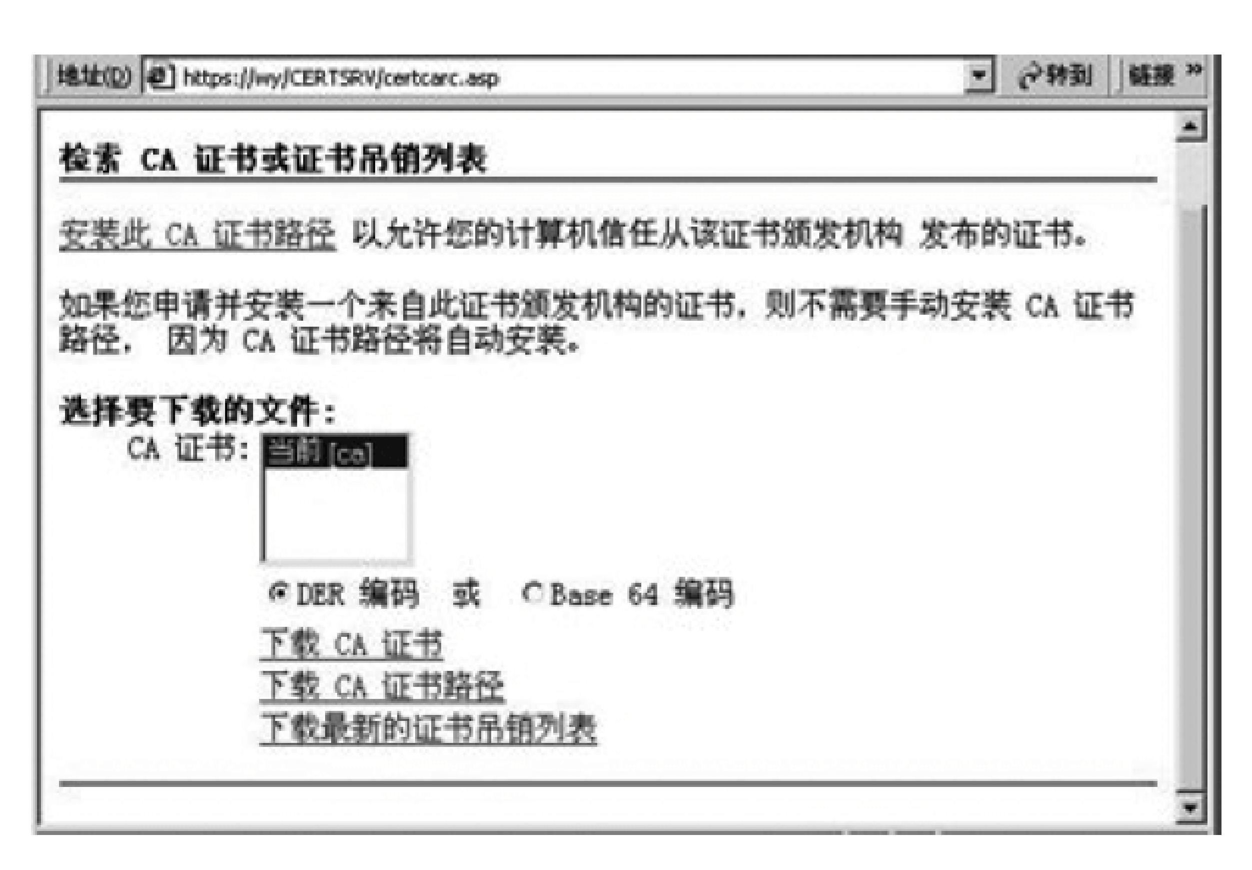


图 3-6-5　证书安装对话框

4. 安装服务器证书

进入 Web 服务器，打开“MyWeb 属性”对话框，单击“服务器证书”，在“IIS 证书向导”对话框中按提示操作即可安装服务器证书。步骤如下。

（1）选择“处理挂起的请求并安装证书”。

（2）输入证书文件名时，单击“浏览”按钮，选择桌面上的文件“mywebcert”（即存储刚才生成的服务器证书的文件），单击“打开”按钮，直到出现“完成”对话框时，单击“完成”按钮即完成证书安装。

5. 实现对 IIS 相关目录的安全访问

在 IIS 相关目录上右击选择“属性”→“目录安全性”，在“匿名访问和验证控制”中选择“匿名访问”，然后在“安全通信”中选择“编辑”，进入如图 3-6-6 所示界面，在选择框中选择“申请安全通道（SSL）”选项，再选择“接收客户证书”选项，如图 3-6-7 所示。

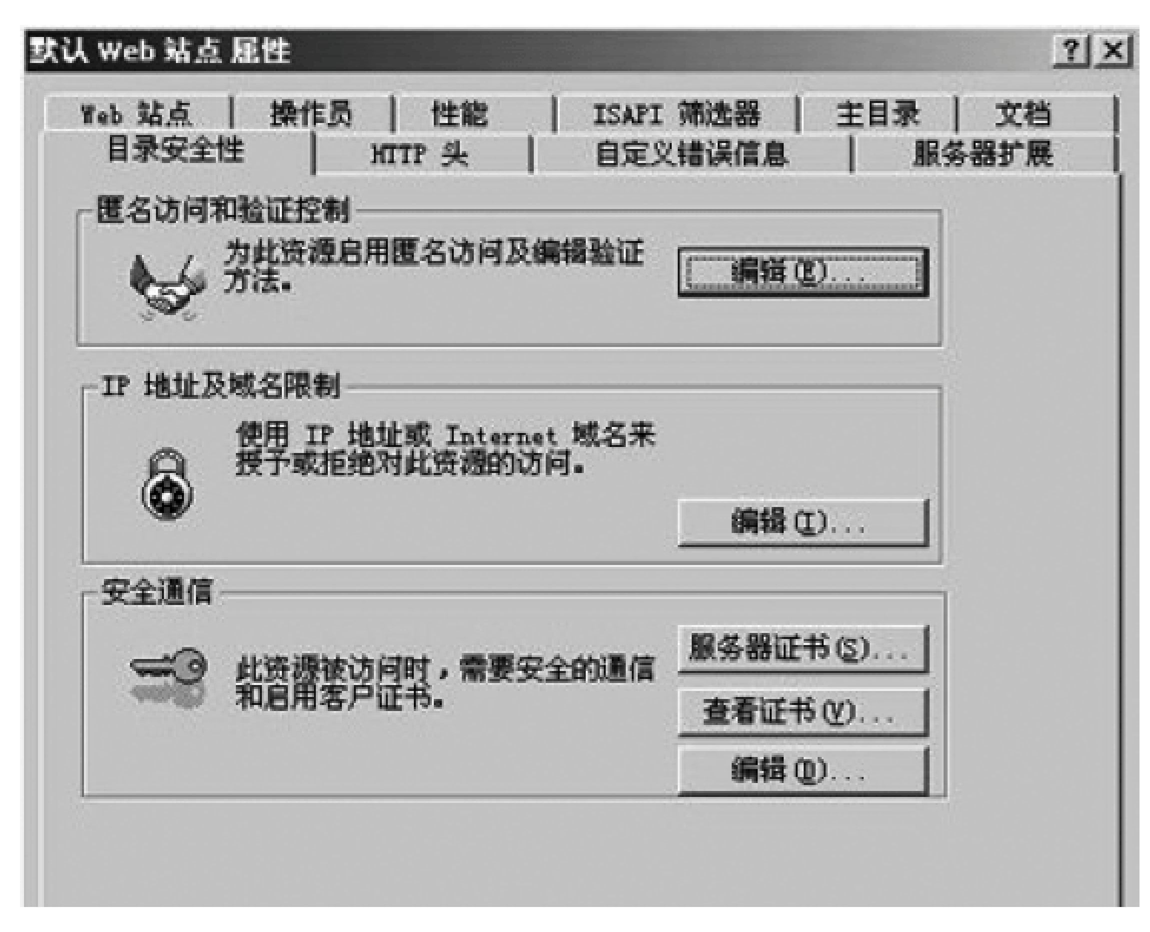


图 3-6-6　目录安全性选项对话框

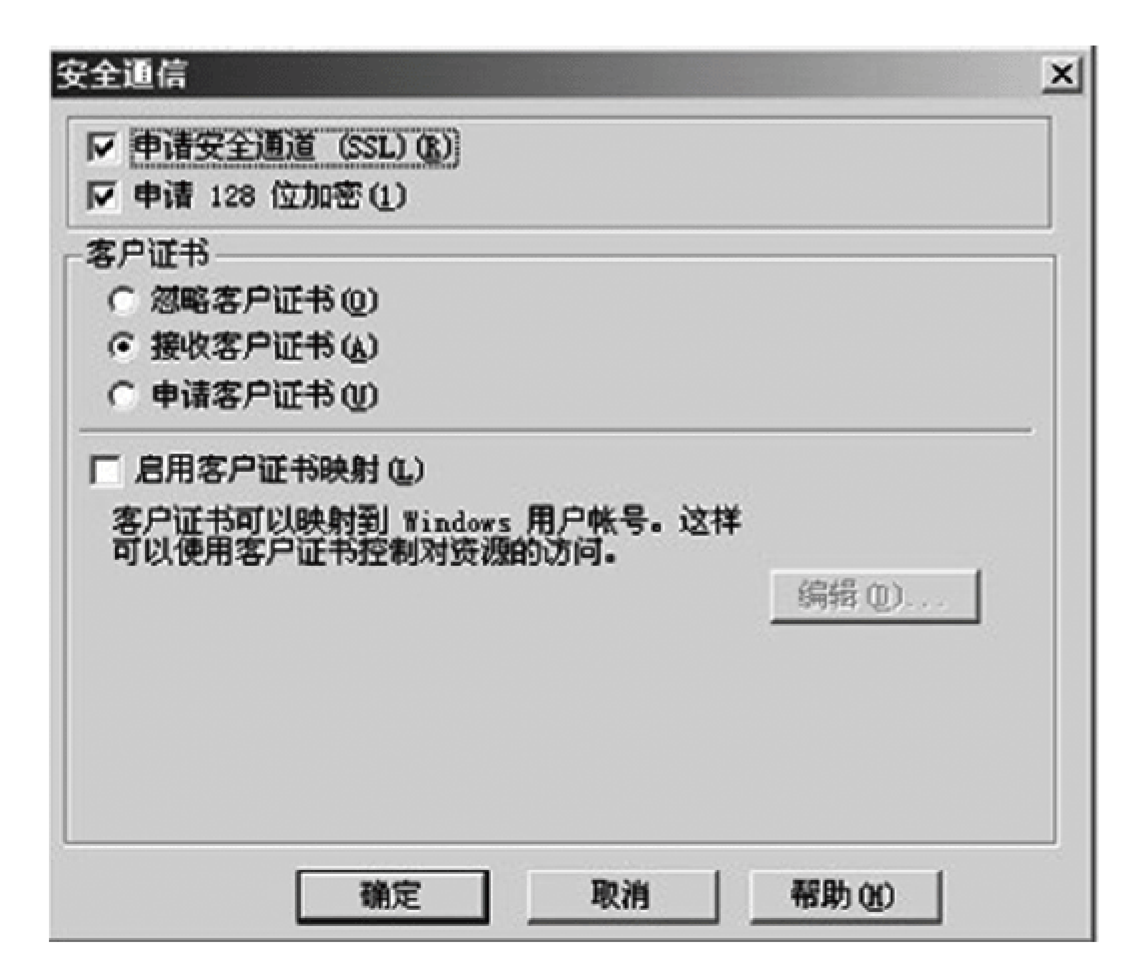


图 3-6-7 “安全通信”对话框

6. 申请并安装客户端证书

在用户申请中有 Web 浏览器证书时，申请和安装的步骤如下。

(1) 启动 IE，在地址栏输入“http://10.0.0.1/certsrv”，进入如图 3-6-4 所示认证申请对话框。

(2) 单击“下一步”按钮，在“用户证书申请”框中选择“Web 浏览器证书”，单击“下一步”按钮，在“标识信息”页面填写相关的信息，单击“提交”按钮，完成客户证书的申请。

(3) 在证书颁发服务器打开“证书颁发机构”，在“待定申请”中将会发现有一新的申请，将其颁发，则完成客户证书的颁发。

(4) 在客户端重新输入“http://10.0.0.1/certsrv”并按 Enter 键，选择“检查挂起的证书”，单击“下一步”按钮，选择要下载的证书，单击“下一步”按钮，选择“安装此证书”，则完成客户证书的安装过程。

7. 使用 https 访问 Web 服务器

(1) 在 Web 服务器上建立并设置默认主页。

(2) 访问安全 Web 的方式如下：在安装了客户证书的主机启动 IE，在地址栏输入 Web 服务器的地址“https://10.0.0.1”，按 Enter 键，在弹出的对话框中选择所申请的证书，即可访问该 Web 服务器。

实验内容二：电子邮件数字证书

硬件环境：主流配置 PC 4 台，以太网交换机 1 台，其网络拓扑结构如图 3-6-8 所示。

操作系统：IP 地址为 192.168.10.10/24 的主机安装 Windows 2000 Pro SP4 操作系统；IP 地址为 192.168.10.11/24 的主机安装 Windows 2000 Server SP4 操作系统，主机名为 www.def.mb；IP 地址为 192.168.10.12/24 的主机安装 RedHat Linux 9.0 操作系统，主机名为 dns.def.mb；IP 地址为 192.168.10.20/24 的主机安装 Windows 2000 Pro SP4 操作系统。

工具手段：伪造电子邮件发送工具 ZapMail.exe，国产电子邮件客户端软件 foxmail6.0beta4.exe。

任务分工：人员A在IP地址为192.168.10.10/24的主机上实现电子邮件接收等任务；人员B在IP地址为192.168.10.11/24的主机上实现配置CA服务器等任务；人员C在IP地址为192.168.10.12/24的主机上实现安装配置Sendmail服务器DNS服务器等任务；人员D在IP地址为192.168.10.20/24的主机上实现进行电子邮件发送等任务。

(1) 人员C安装配置DNS服务器。新建一个终端，输入命令“redhat-config-packages”后按Enter键，在添加删除程序中选择DNS Name Server，然后单击Update按钮更新，如图3-6-9所示。

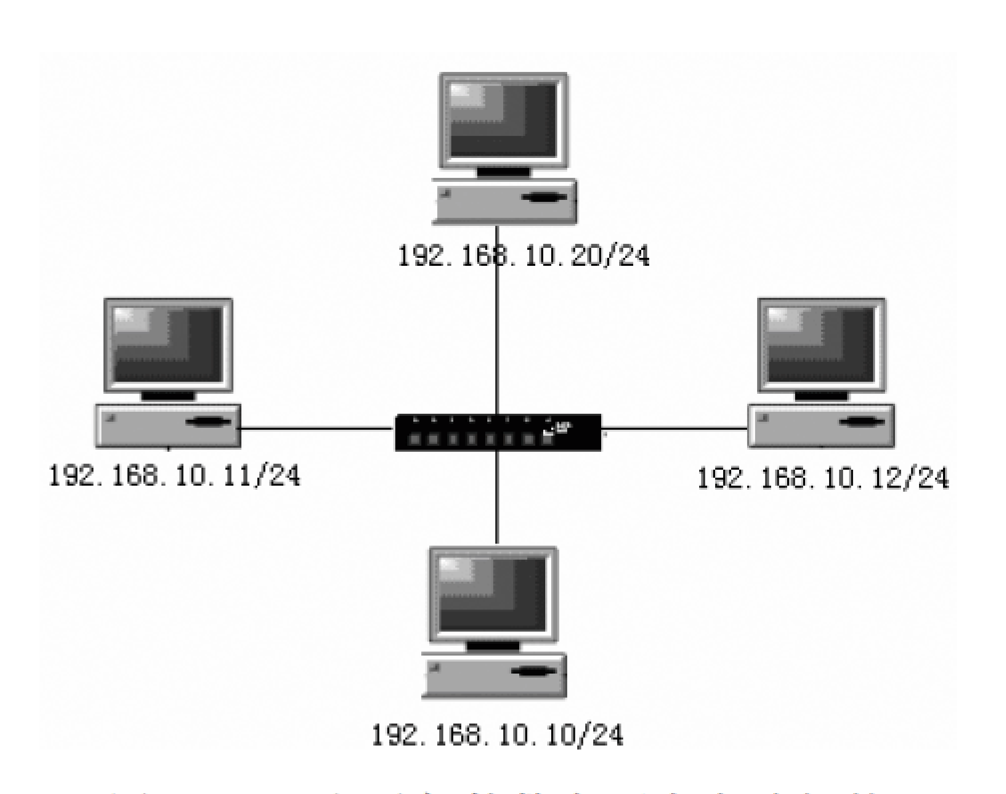


图3-6-8 电子邮件数字证书实验拓扑

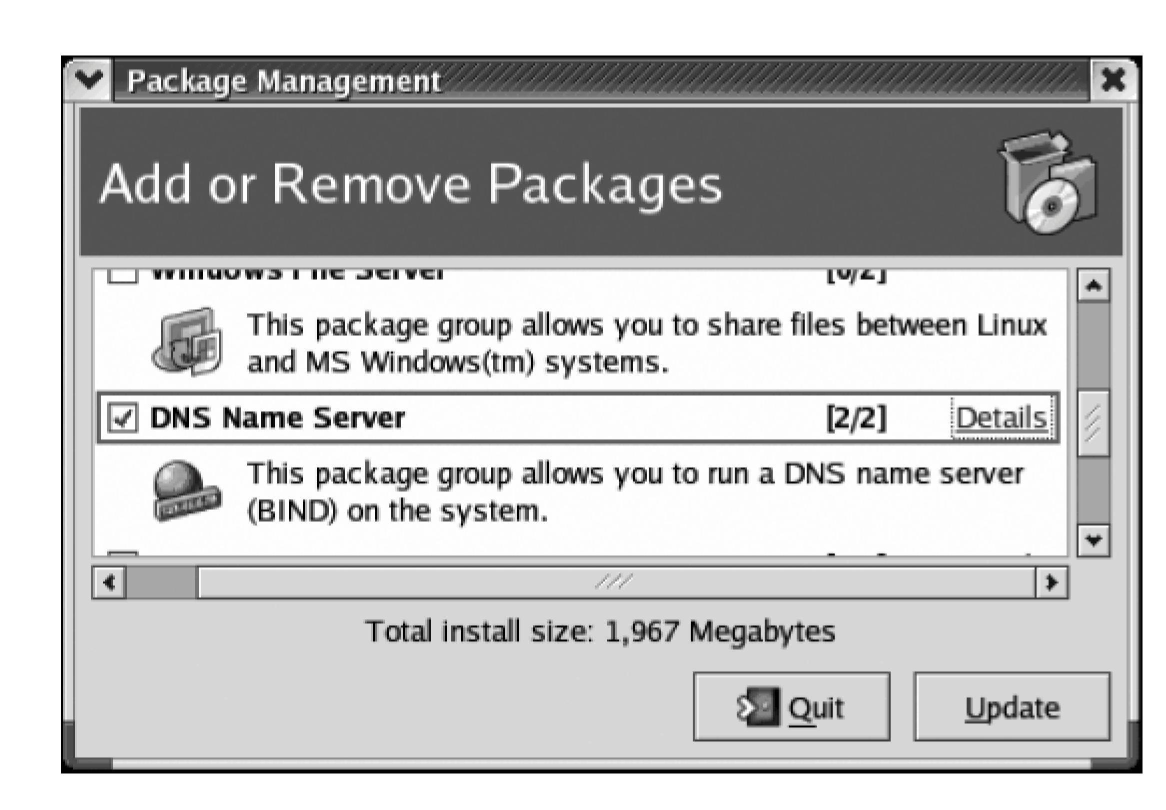


图3-6-9 安装DNS服务器软件包

(2) 使用如下命令启动DNS服务。

```
#service named start
#chkconfig named--level 35 on
```

(3) 打开文件/etc/named.conf，添加如下内容建立域def.mb。其正向解析文件为def.mb.zone，反向解析文件为def.mb.arpa，网络地址为192.168.10.0/24。

```
//////begin config the zone of def.mb//////
zone "def.mb"IN{
    type master;
    file "def.mb.zone";
};
zone "10.168.192.in-addr.arpa" IN{
    type master;
    file "def.mb.arpa";
};
```

(4) 在/var/named/目录下新建文件def.mb.zone，内容如下：

```
$ TTL     86400
@         IN SOA def.mb.     root@ dns.def.mb.(
                42           ;serial(d. adams)
                3H           ;refresh
                15M          ;retry
```

```
                1W          ;expiry
                1D)         ;minimum

           IN NS        def.mb.
@          IN MX 1          mail
dns        IN A             192.168.10.12 mail
           IN A         192.168.10.12
www            IN A     192.168.10.11
```

(5) 在/var/named/目录下新建文件 def.mb.arpa,内容如下:

```
$TTL    86400
@       IN     SOA     localhost. root.localhost.  (
                                       1997022700 ;Serial
                                       28800      ;Refresh
                                       14400      ;Retry
                                       3600000    ;Expire
                                       86400)     ;Minimum
@              IN     NS     localhost.

12     IN     PTR     dns.def.mb.
12     IN     PTR     mail.def.mb.
11     IN     PTR     www.def.mb.
```

(6) 重新启动 DNS 服务:

```
#service named reload
```

(7) 人员 A 在 IP 地址为 192.168.10.10/24 的主机上实现将 DNS 服务器的 IP 地址设置为 192.168.10.12,如图 3-6-10 所示。

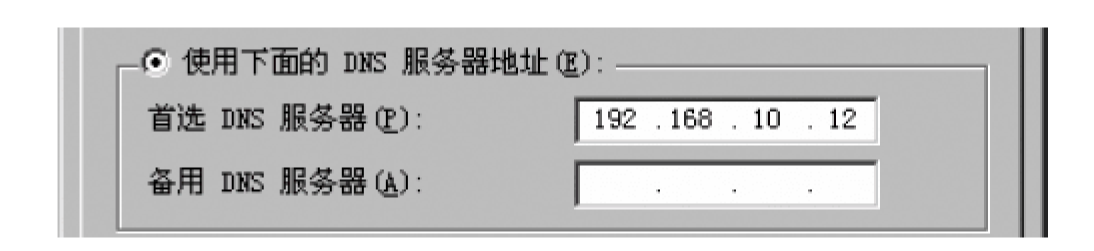


图 3-6-10 设置 DNS 服务器的地址

(8) 在命令提示符下运行如图 3-6-11 所示命令以验证 DNS 服务器是否可以正常工作。

```
nslookup
```

(9) 人员 C 安装配置 Sendmail 服务器。新建一个终端,输入命令"redhat-config-packages"后按 Enter 键,在添加删除程序中选择 Mail Server,如图 3-6-12 所示,单击 Details 确保 imap 和 sendmail-cf 选中,然后更新,如图 3-6-13 所示。

(10) 使用如下命令启动 sendmail,看到 OK 后确认服务已经启动。

```
#service sendmail start
#chkconfig sendmail--level 35 on
```

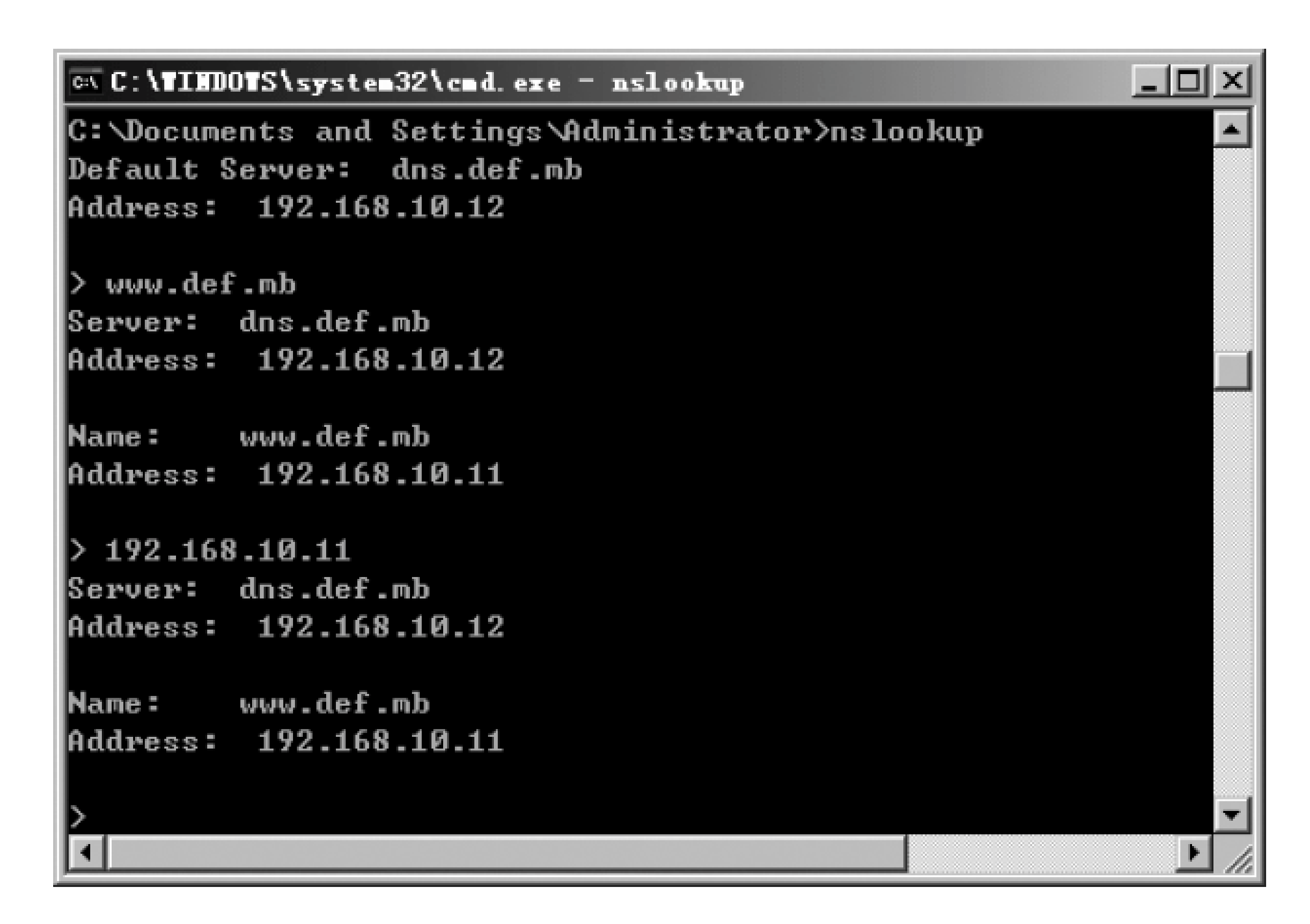


图 3-6-11 验证 DNS 服务

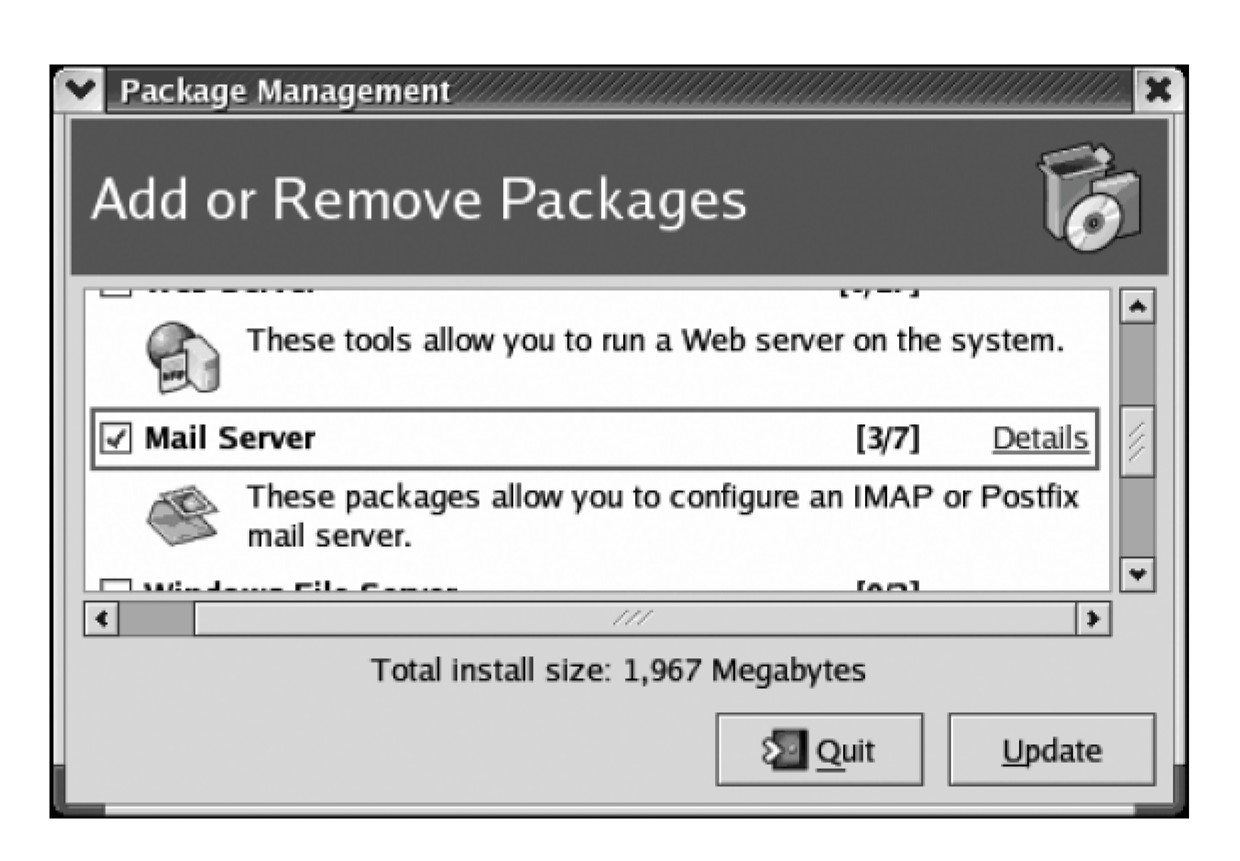


图 3-6-12 安装 Mail Server 服务器软件包

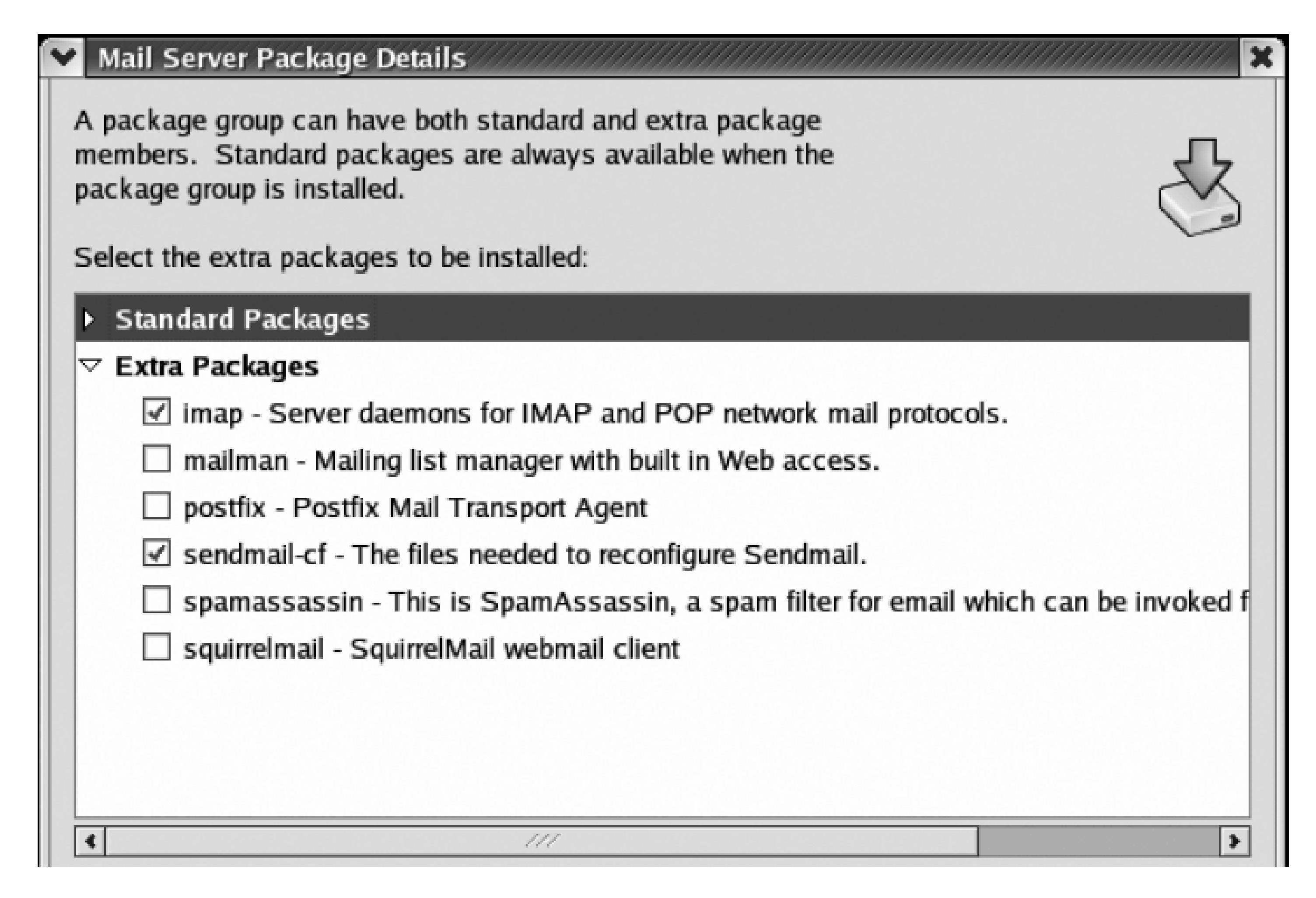


图 3-6-13 选择 Mail Server 服务器软件包

(11) 修改/etc/mail/sendmail.cf 文件来配置 sendmail 的监听端口:

```
#SMTP daemon options
O DaemonPortOptions=Port=smtp,Addr=127.0.0.1,Name=MTA
```

更改为:

```
O DaemonPortOptions=Port=smtp,Addr=192.168.10.12,Name=MTA
```

改完后保存退出,并且重新启动 sendmail 服务:

```
#service sendmail restart
```

使用如下命令检查 sendmail 服务,出现 192.168.10.12:25 说明服务已经在运行:

```
#netstat -ant
```

(12) 修改/etc/xinetd.d/下面的 ipop3 和 imap 文件,把 disable 的值改为 no,重新加载配置文件使它生效:

```
#/service xinetd reload
```

(13) 在/etc/mail/access 文件中加入下面一行:

```
def.mb        RELAY
```

保存后运行 make access.db 的命令来生成 access.db 文件。

```
#cd/etc/mail
#make access.db
```

(14) 修改/etc/mail/local-host-nameds 文件:

```
#vi local-host-names
//添加如下两行
mail.def.mb
def.mb
```

(15) 重新启动:

```
#services sendmail restart
```

(16) 在 mail 组中增加用户并且设置密码为 123456:

```
#useradd -g mail alice
#passwd alice 按 Enter 键后输入密码
123456
```

按 Enter 键后再次输入确认。

```
#useradd -g mail bob
#passwd bob 按 Enter 键后输入密码
123456
```

按 Enter 键后再次输入确认。

(17) 人员 A 在 IP 地址为 192.168.10.10/24 的主机上实现打开光盘中的电子邮件客户端软件 foxmail6.0beta4.exe,双击安装。

(18) 新建一个邮箱账户 alice@mail.def.mb,账户密码是 123456,如图 3-6-14 所示。

(19) 人员 D 在 IP 地址为 192.168.10.20/24 的主机上实现打开光盘中的电子邮件客户端软件 foxmail6.0beta4.exe,双击安装。

(20) 新建一个邮箱账户 bob@mail.def.mb,账户密码是 123456,如图 3-6-15 所示。



图 3-6-14 账户 alice 的邮箱



图 3-6-15 账户 bob 的邮箱

(21) 人员 D 将其 DNS 设置为 192.168.10.12。

(22) 人员 A 和人员 D 互相发一封邮件,并接收对方发来的邮件,以确认邮件服务器可以工作。

(23) 人员 D 打开光盘中的伪造电子邮件发送工具 ZapMail.exe,双击运行,将如图 3-6-16 所示的内容填写完毕,并单击 Send 按钮。在这里伪造了一个来源为 test@mail.def.mb 的邮件地址。



图 3-6-16 人员 D 伪造电子邮件

(24) 人员 A 接收邮件,他不能确认邮件内容的真实性。

(25) 人员 B 在 IP 地址为 192.168.10.11/24 的主机上配置 CA 服务器。选择"控制面板"→"添加/删除程序"→"添加/删除 Windows 组件",在可选项中选择"证书服务",单击"详细信息",确保"证书服务 Web 注册支持"和"证书服务颁发机构(CA)"都被选中,并开始安装。安装过程中,证书颁发的类型选择"独立根 CA"。进入下一步安装,填写 CA 的相关信息,如图 3-6-17 所示。

(26) 单击"下一步"按钮,选择证书数据库及日志的位置,确认后继续进行安装。

(27) 安装结束后,选择"开始"→"设置"→"控制面板"→"管理工具",双击"证书颁发机构",如图 3-6-18 所示。

(28) 单击 CA 名称,选择"属性"→"策略模块"→"配置",选择"证书申请设为待定,系统管理员必须专门颁发证书",这样管理员就可以直接控制证书的发放了。

(29) 对于相关的申请,都可以在"证书颁发机构"→"待定申请"中看到,选择相应的申请,右击,选择"颁发"或"拒绝"选项。如果要吊销证书,可以在"证书颁发机构"→"已颁发证书"选项中选择相应证书,右击,可以进行"吊销证书"的操作。对于吊销的证书,也可

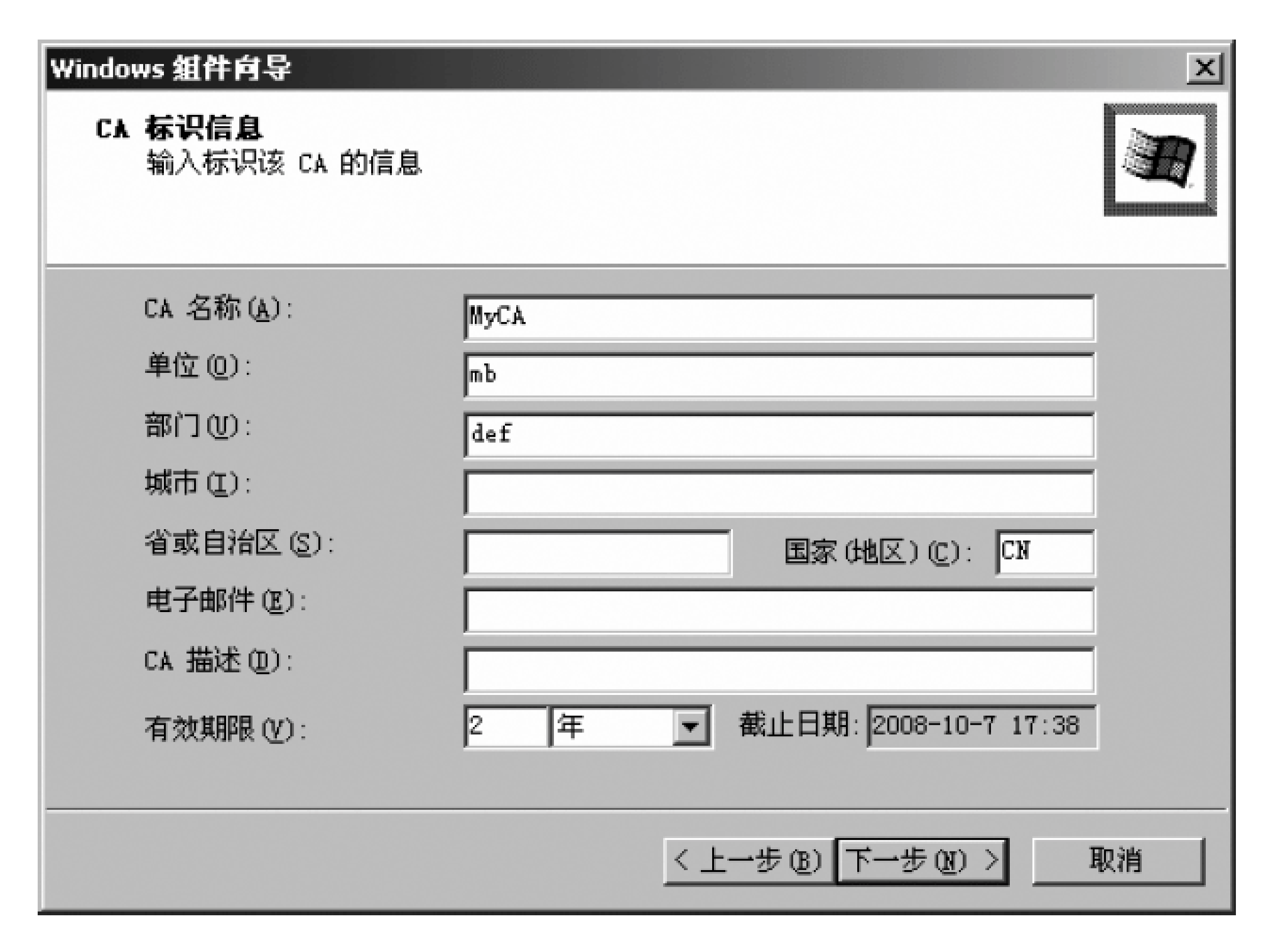


图 3-6-17　填写 CA 标识信息

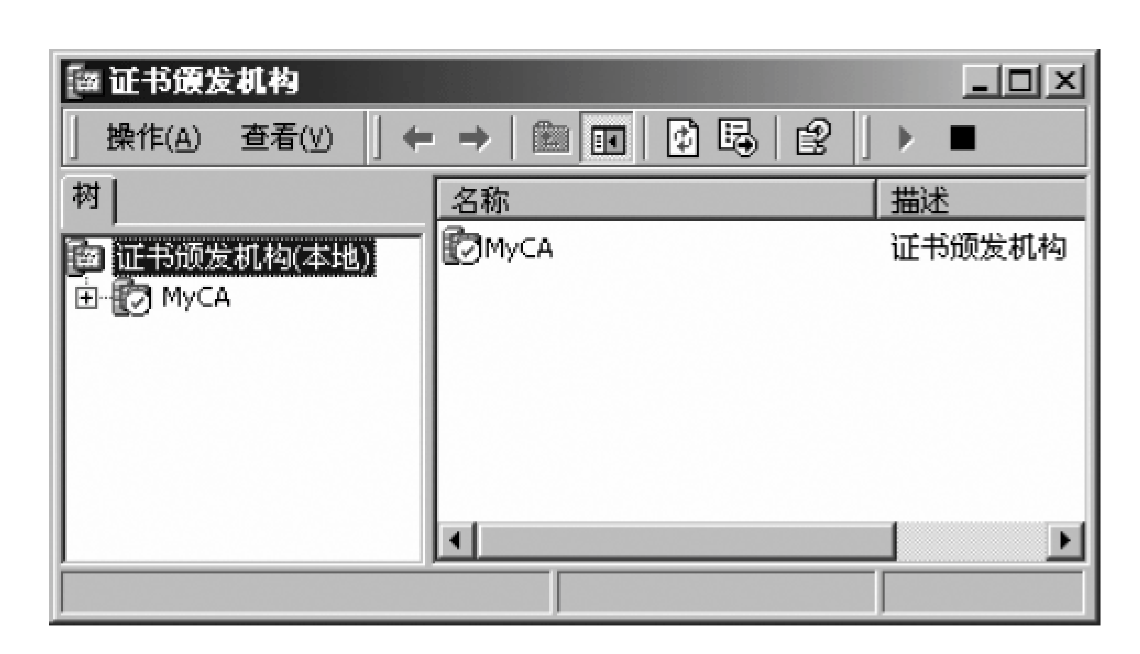


图 3-6-18　证书颁发机构

以在“证书颁发机构”→“吊销的证书”中选择相应的证书，右击，选择“重新颁发证书”。

(30) 人员 A 申请电子邮件证书。启动 IE，在地址栏输入地址 http://192.168.10.11/certsrv 并按 Enter 键。

(31) 在欢迎页面上选择任务为“申请证书”，单击下一步，在选择申请类型页面上单击“电子邮件保护证书”，单击下一步，在标识信息页面上填入申请者的信息。填写完毕后单击“提交”，如图 3-6-19 所示。



图 3-6-19　填写标识信息

(32) 人员B打开“证书颁发机构”,可以看到在“待定申请”中有一个新的申请,选择相应的申请,右击选择“颁发”,则生成了相应的电子邮件证书。

(33) 人员A在IE地址栏输入地址 http://192.168.10.11/certsrv 并按 Enter 键,在欢迎页面上选择“检查挂起的证书”,单击“下一步”,在检查挂起的证书申请页面上单击将要下载的证书,如图3-6-20所示,并单击“下一步”。

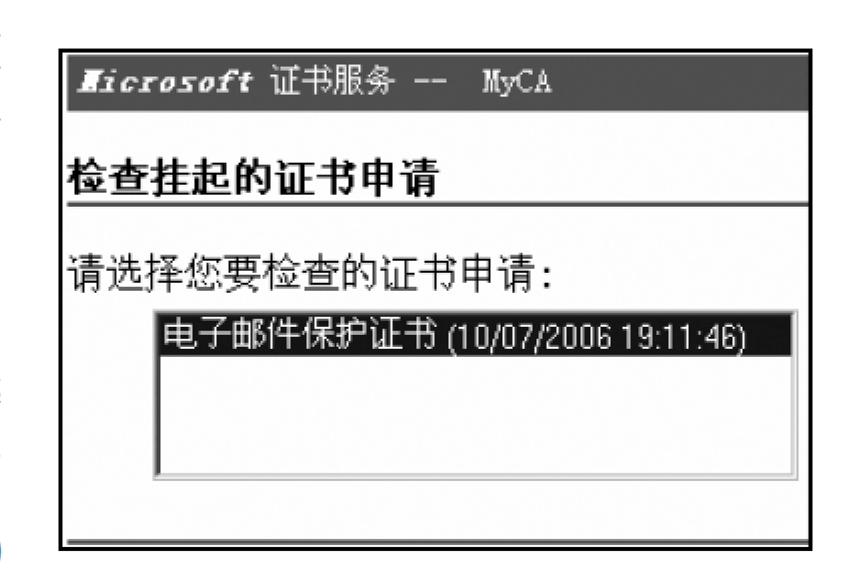


图 3-6-20 检查挂起的证书

(34) 在证书已发布页面单击“安装此证书”,完成证书的安装。

(35) 人员D重复此过程完成电子邮件证书的申请和安装。

(36) 人员A打开 foxmail 窗体,在 alice@mail.def.mb 邮箱账户上右击,然后单击“属性”,在邮箱账户设置窗体上单击“安全”,然后单击安全属性窗体中的“选择”按钮,如图3-6-21所示。



图 3-6-21 设置安全属性并选择证书

(37) 在弹出的窗体中选择电子邮件证书,并单击“确定”按钮,在邮箱账户设置窗体上单击“确定”按钮完成电子邮件证书的安装,如图3-6-22所示。

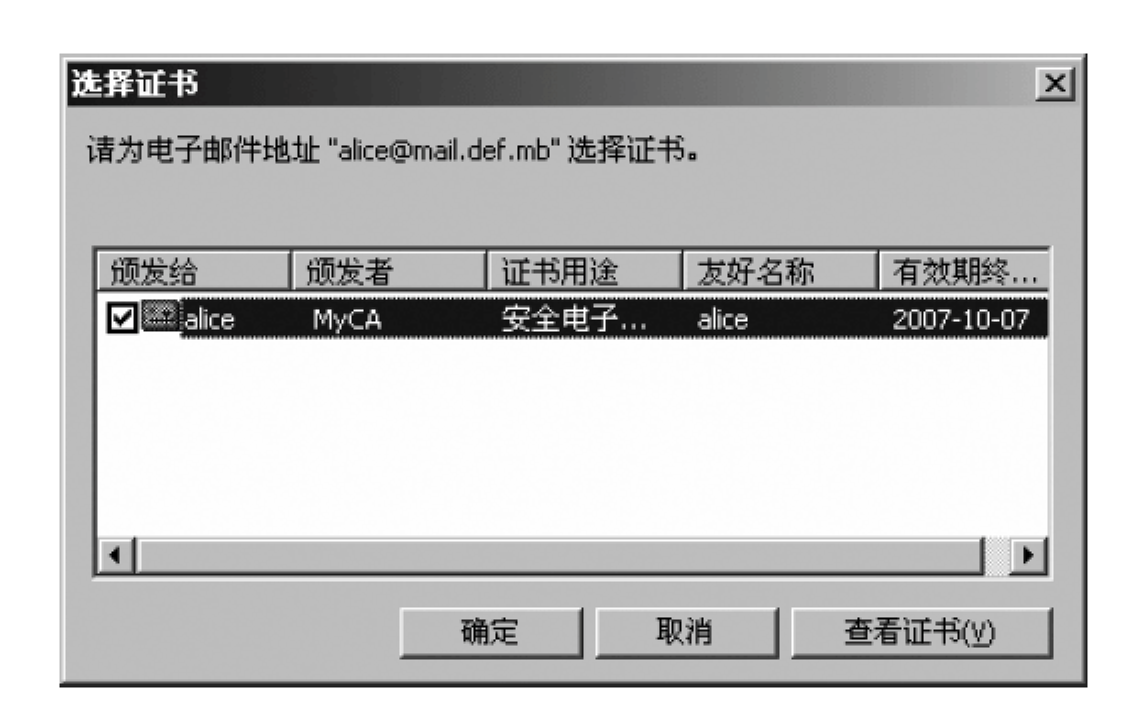


图 3-6-22 选择电子邮件证书

(38) 人员 D 重复以上过程完成 bob@mail.def.mb 邮箱证书的安装。

(39) 人员 A 打开 foxmail 电子邮件客户端,在工具栏中单击“撰写新邮件”,收件人为 bob@mail.def.mb,主题为 I am Alice,内容为 This is a test。单击工具栏的“选项”,然后在菜单中单击选择“数字签名”,然后单击工具栏的“发送”。

(40) 人员 D 打开 foxmail 电子邮件客户端,在工具栏中单击“收取”,单击收到的邮件,将看到签名信息的提示,单击“继续”按钮,看到图 3-6-23 所示内容。



图 3-6-23 邮件内容

(41) 单击右上角的符号,将显示签名信息,可以看到数字签名方为 alice,此外还可以单击“查看签名证书”按钮查看详细的证书信息。因为每个邮件地址只能使用一个证书,所以任何伪造发信人地址的邮件都由于缺少相应的证书而难以奏效,如图 3-6-24 所示。

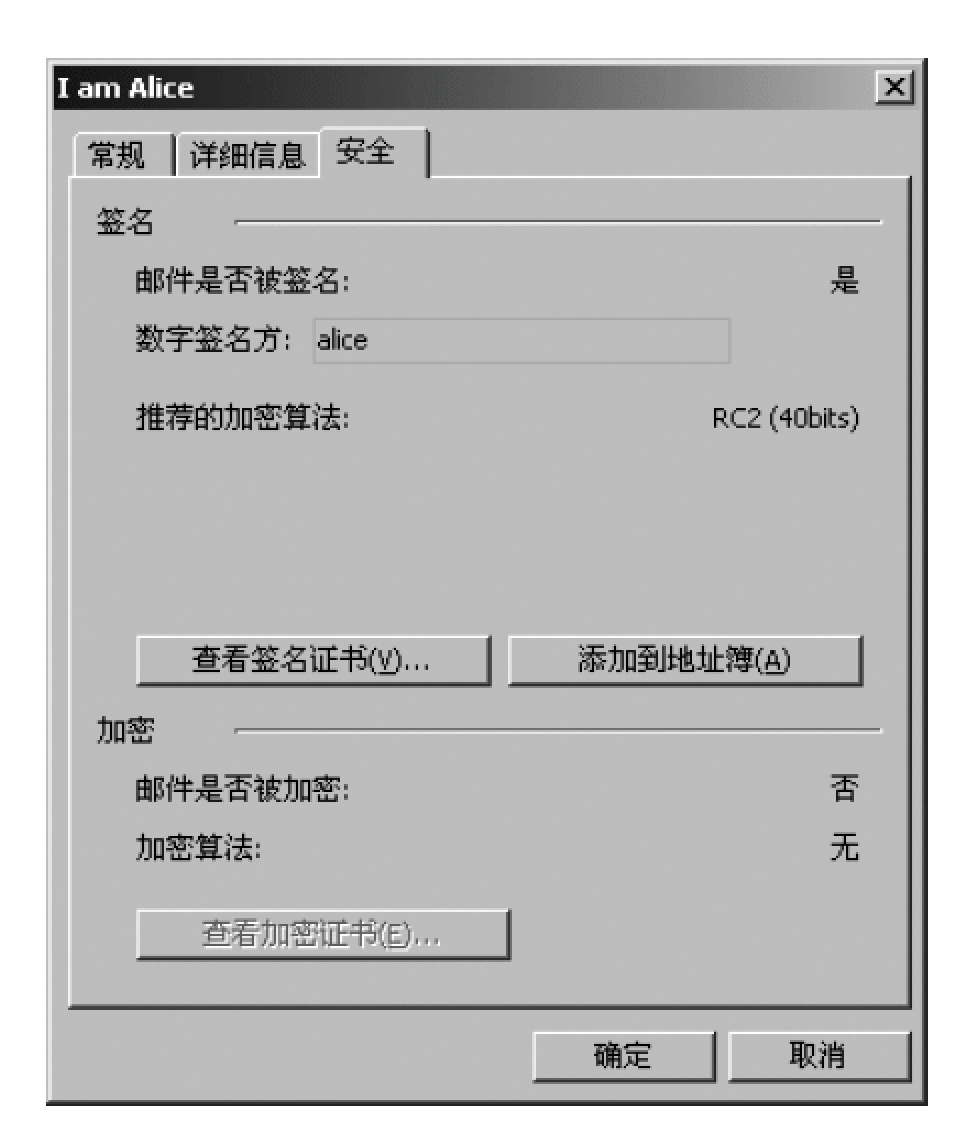


图 3-6-24 显示签名信息

3.6.8 实验思考

1. 建立认证中心(CA)应考虑哪些方面的问题?
2. 电子邮件的加密功能和认证功能有哪些异同?

3.7 访问控制和网络防火墙

3.7.1 实验类型

综合型,8学时,必选实验。

3.7.2 实验目的

访问控制是网络安全防范和保护的主要核心策略,它的主要任务是保证网络资源不被非法使用和访问。通常将访问控制技术划分为如下几个方面:入网访问控制、网络权限控制、目录级安全控制、属性安全控制以及网络服务器的安全控制等。通过实验,使学生认识网络访问控制的内容,掌握网络访问控制的方法。

3.7.3 题目描述

使用网络防火墙联想网御2000进行网络访问控制。

3.7.4 实验要求

理解访问控制的内涵,认识访问控制对信息安全保障的影响。能够根据访问控制需求使用联想网御2000进行网络访问控制。

提高要求:能够对Windows NTFS文件系统进行权限分配。

3.7.5 相关知识

1. 访问控制

访问控制是网络安全防范和保护的主要核心策略,它的主要任务是保证网络资源不被非法使用和访问。访问控制规定了主体对客体访问的限制,并在身份识别的基础上,根据身份对提出资源访问的请求加以控制。它是对信息系统资源进行保护的重要措施,也是计算机系统最重要和最基础的安全机制。

访问控制的基本概念如下。

1) 主体(Subject)

主体是指主动的实体,是访问的发起者,它造成了信息的流动和系统状态的改变。主体通常包括人、进程和设备。

2) 客体(Object)

客体是指包含或接受信息的被动实体,客体在信息流动中的地位是被动的,是处于主体的作用之下,对客体的访问意味着对其中所包含信息的访问。客体通常包括文件、设

备、信号量和网络节点等。

3）访问(Access)

访问(Access)是使信息在主体(Subject)和客体(Object)之间流动的一种交互方式。

4）访问控制(Access Permissions)

访问控制决定了谁能够访问系统，能访问系统的何种资源以及如何使用这些资源。适当的访问控制能够阻止未经允许的用户有意或无意地获取数据。访问控制的手段包括用户识别代码、口令、登录控制、资源授权(例如用户配置文件、资源配置文件和控制列表)、授权核查、日志和审计等。

2. 访问控制策略

访问控制涉及的领域很广，方法也很多，通常访问控制策略可以划分为自主访问控制(Discretionary Access Control)、强制访问控制(Mandatory Access Control)和基于角色的访问控制(Role Based Access Control)3 种。

3. 访问控制的方法

(1) 网络访问控制，主要包括 MAC 地址过滤、VLAN 隔离、IEEE 802.1Q 身份验证、基于 IP 地址的访问控制列表和防火墙控制等。

(2) 目录级安全控制，如 Windows 的 NTFS 文件系统，Linux 的 EXT3 文件系统，可以根据系统用户的身份对系统文件目录进行详细的访问权限设置。

(3) 属性安全控制，设置文件或目录的读、写、隐藏等属性。

(4) 网络服务器的安全控制，如设置服务访问口令等。

4. 防火墙的分类

防火墙从实现方式上，可以分为软件防火墙、硬件防火墙和嵌入式防火墙三类。软件防火墙运行于特定的计算机上，它需要预先安装好的计算机操作系统的支持(如 Linux，UNIX 或 Windows 2000)，一般来说这台计算机就是整个网络的网关，如天网个人及企业版防火墙、Norton 个人及企业版软件防火墙以及 Linux 防火墙等。

硬件防火墙如果从技术上又可分为两类：标准防火墙和应用层网关防火墙。标准防火墙系统包括一个 UNIX 工作站，该工作站的两端各连接一个路由器进行缓冲。其中一个路由器的接口是外部世界，即公用网；另一个则连接内部网。标准防火墙使用专门的软件，并要求较高的管理水平，而且在信息传输上有一定的延迟。应用层网关(applications layer gateway)又称堡垒主机，是一个单个的系统，却能同时完成标准防火墙的所有功能。其优点是能运行更复杂的应用，同时防止在互联网和内部系统之间建立任何直接的边界，可以确保数据包不能直接从外部网络到达内部网络，反之亦然。

嵌入式防火墙通常指的是防火墙功能被集成到路由器或者交换机中的防火墙，这类防火墙在进行数据包检测路由器的时候，先检测包的安全性，再进行路由。这里说的硬件防火墙区别于嵌入式防火墙，设计为一种总体系统。根据是否基于专用的硬件平台，嵌入式防火墙又可以分为普通的硬件防火墙和芯片级的硬件防火墙。市面上较常见的普通的硬件防火墙一般基于 PC 架构，在这些 PC 架构计算机上运行一些经过裁剪和简化的操作

系统，本书的实例 FOUND Secuway 100 即属于这一类。芯片级防火墙基于专门的硬件平台，专有的 ASIC 芯片使它们比其他种类防火墙速度更快，性能更高，使用专用的操作系统，防火墙本身的漏洞少。例如 CISCO 的 PIX 防火墙等，就是通过专有技术的硬件和软件的结合来达到隔离内、外部网络的目的。

随着防火墙技术的发展，在应用层网关的基础上又演化出两种防火墙配置，一种是隐蔽主机网关，另一种是隐蔽智能网关(隐蔽子网)。隐蔽主机网关是当前的一种常见的防火墙配置，顾名思义，这种配置一方面将路由器进行隐蔽，另一方面在互联网和内部网之间安装堡垒主机。堡垒主机装在内部网上，通过路由器的配置，使该堡垒主机成为内部网与互联网进行通信的唯一系统。目前技术最为复杂而且安全级别最高的防火墙是隐蔽智能网关，它将网关隐藏在公共系统之后使其免遭直接攻击。隐蔽智能网关提供了对互联网服务几乎透明的访问，同时阻止了外部未授权访问对专用网络的非法访问。一般来说，这种防火墙是最不容易被破坏的。

从对数据包的检测方式，可以把防火墙分为如下三类。

(1) 分组过滤防火墙：不检查数据区，不建立连接状态表，前后报文无关，应用层控制很弱。

(2) 应用网关防火墙：不检查 IP、TCP 报头，不建立连接状态表，网络层保护比较弱。

(3) 状态检测防火墙：不检查数据区，建立连接状态表，前后报文相关，应用层控制很弱。

3.7.6 实验设备

主流配置 PC 一台，Windows 操作系统，联想网御 2000 网络防火墙一台，天网桌面防火墙。

3.7.7 实验步骤

(1) 安装实验所需要的软件 GNS3-0.8.3.1-all-in-on，如图 3-7-1 所示。



图 3-7-1 软件安装

完成 GNS3 安装后的界面如图 3-7-2 所示。

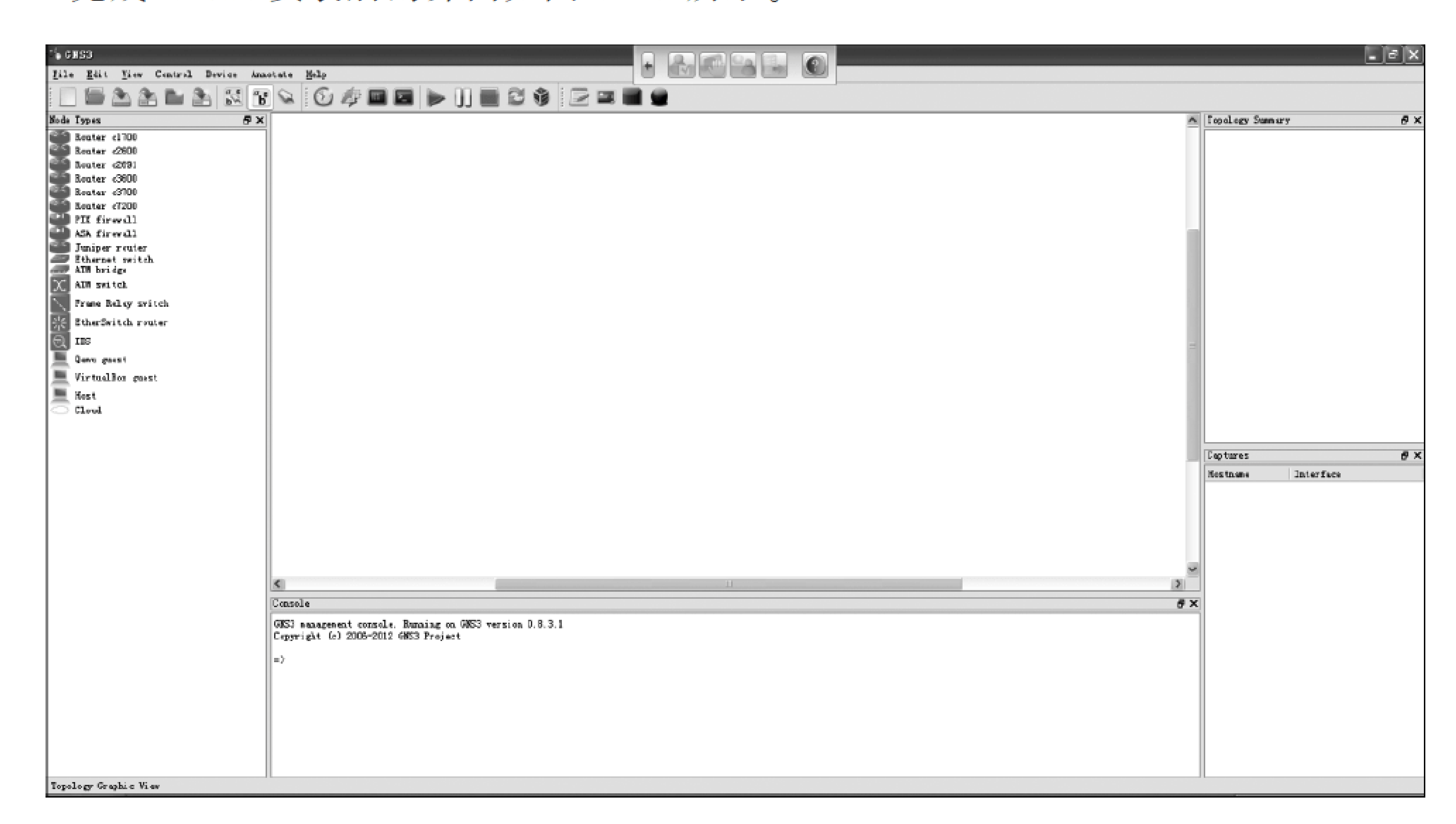


图 3-7-2 安装后界面

图 3-7-2 中的界面是英文的，不便于操作，可将其换成中文的，单击 Edit→Preferences，在语言选框中单击“中国的”，单击 apply 按钮，再单击 OK 按钮，重启 GNS3 后可看到 GNS3 界面变成中文版的，如图 3-7-3 所示。



图 3-7-3 中文版界面

（2）画出基于 GNS 的 PIX 防火墙的实验拓扑图。

① 在菜单栏选择“编辑”→“首选项”→Qemu→PIX，选择 pix804. bin 文件，如图 3-7-4 所示。

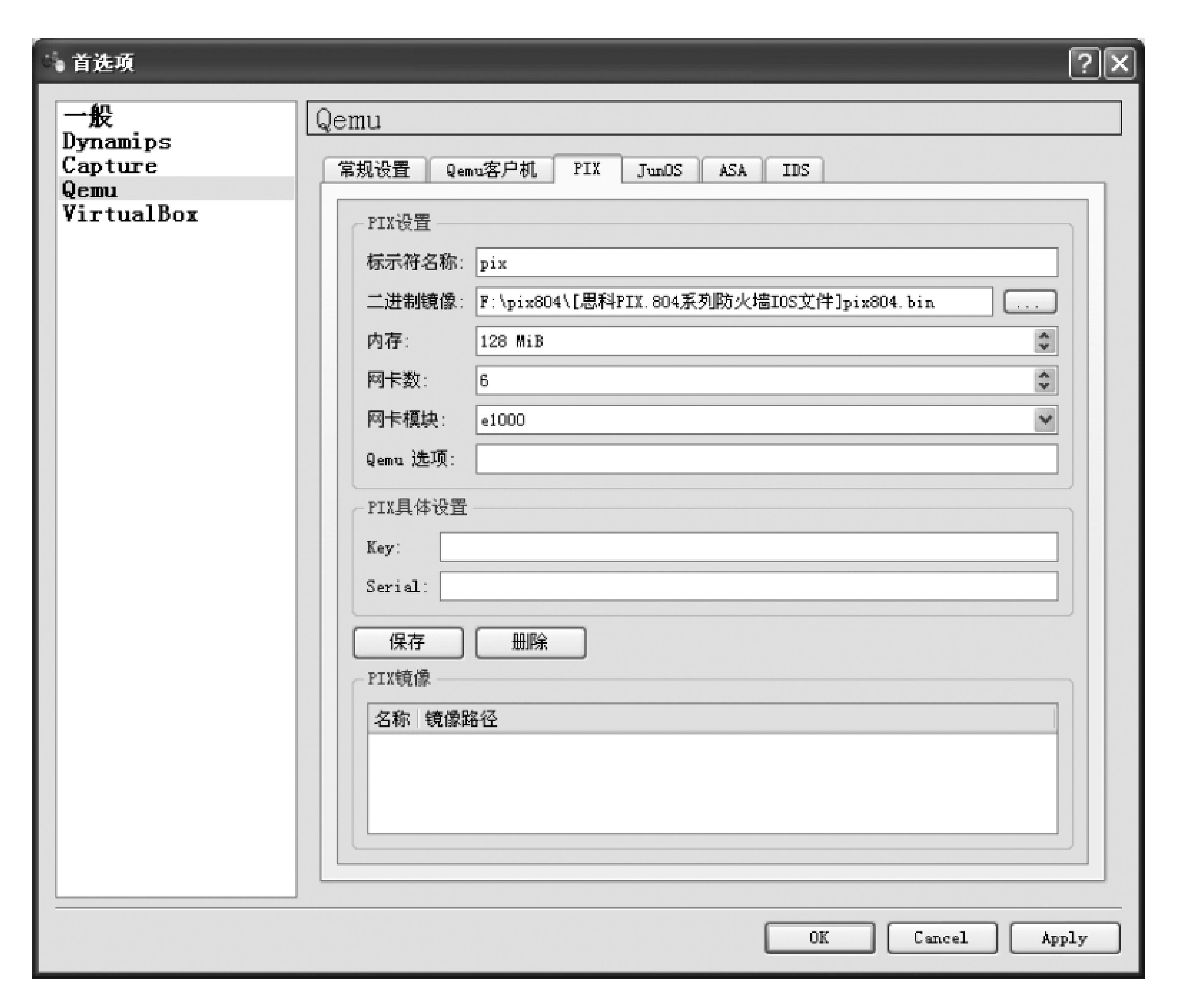


图 3-7-4　PIX 选项卡

② 选择"编辑"→"标示符管理器"→computer,添加 Computer,"类型"选择 Cloud,如图 3-7-5所示。

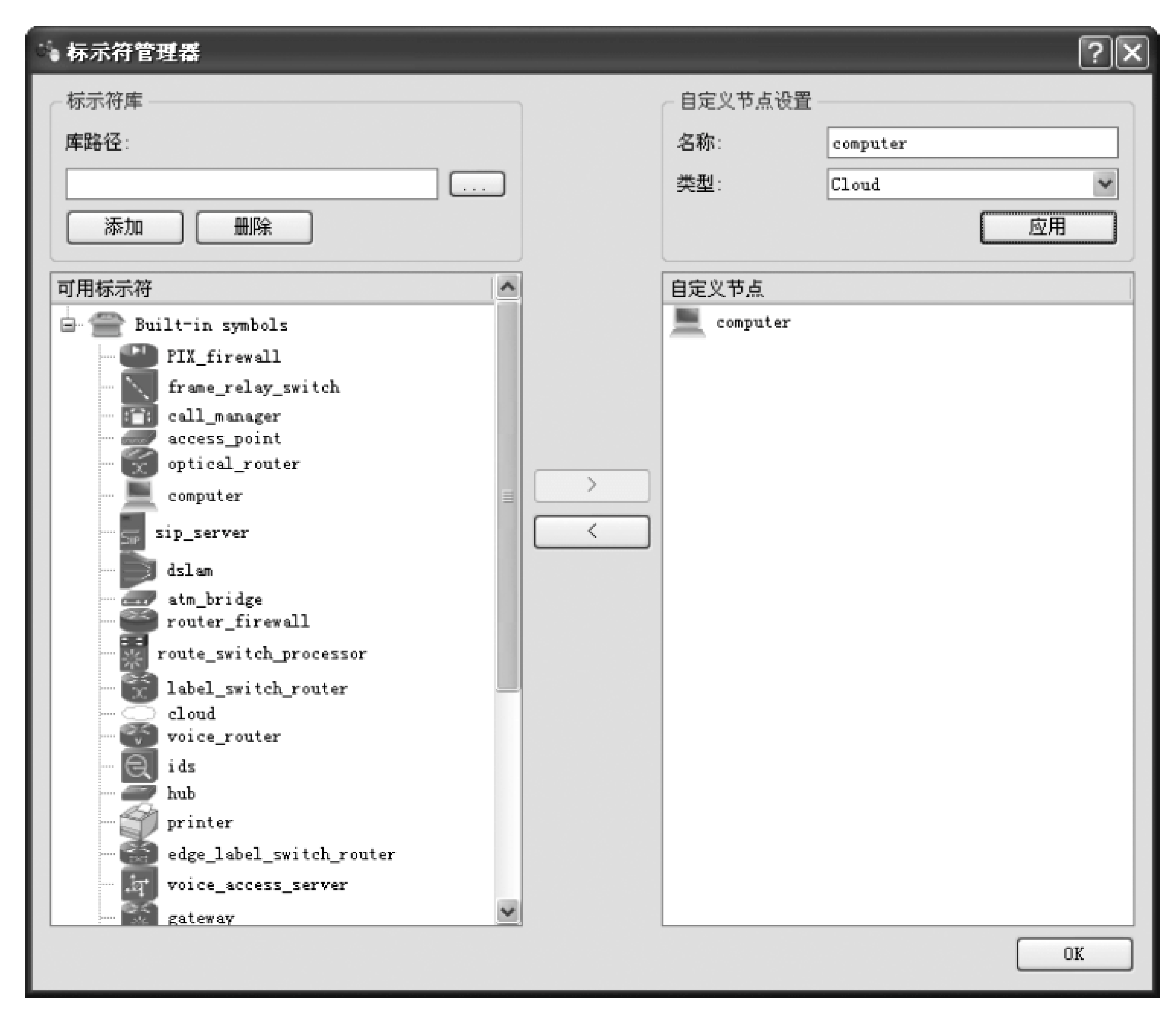


图 3-7-5　添加 Computer

③ 为 router c3700 添加镜像文件 unzip-c3725-adventerprisek9-mz. 124-15. T5，如图 3-7-6所示。

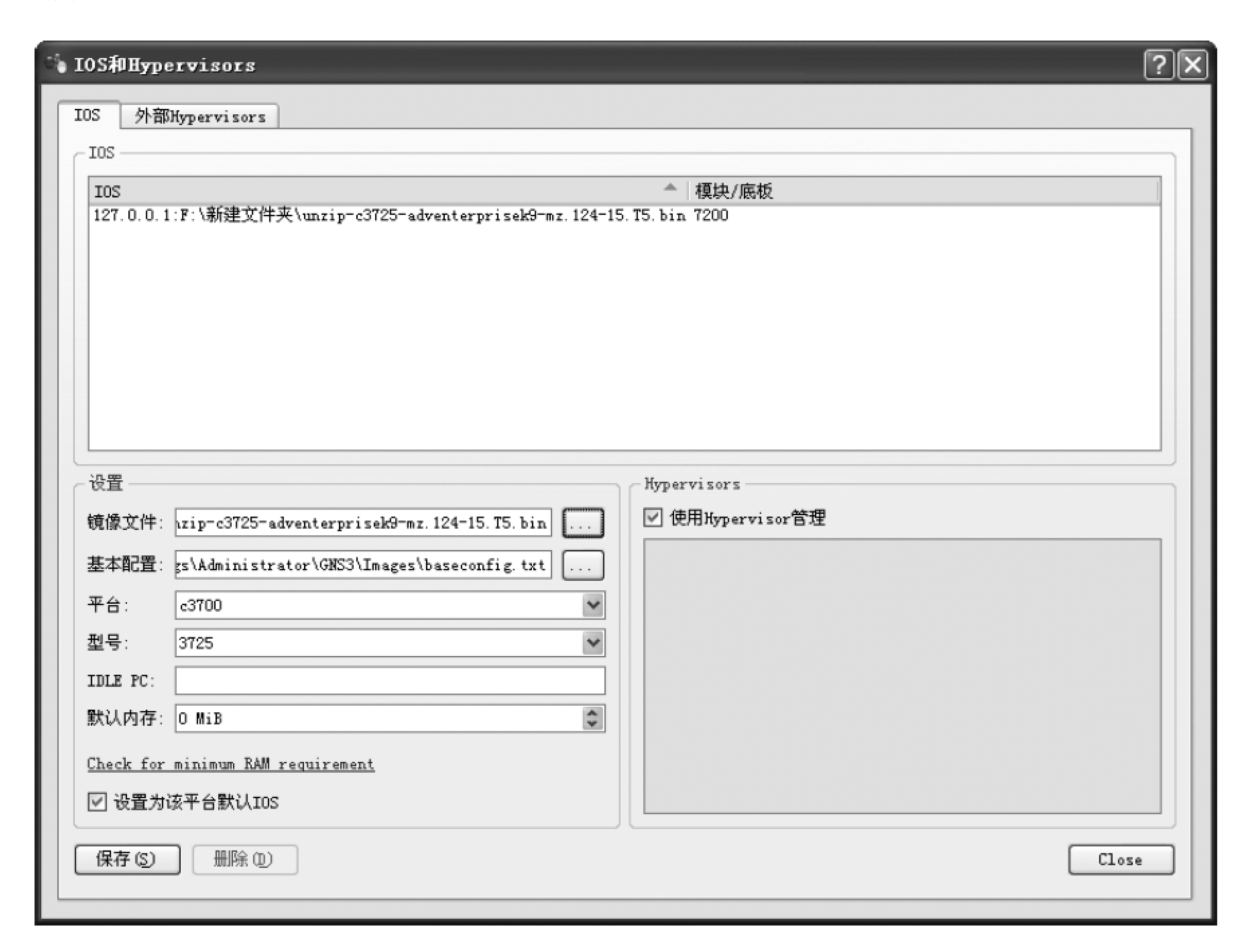


图 3-7-6　添加镜像文件

④ 对 C1 进行配置：右击 C1 图标，选中“配置”→NIO UDP，进行设置后，单击“添加”按钮后单击 OK 按钮，如图 3-7-7 所示。

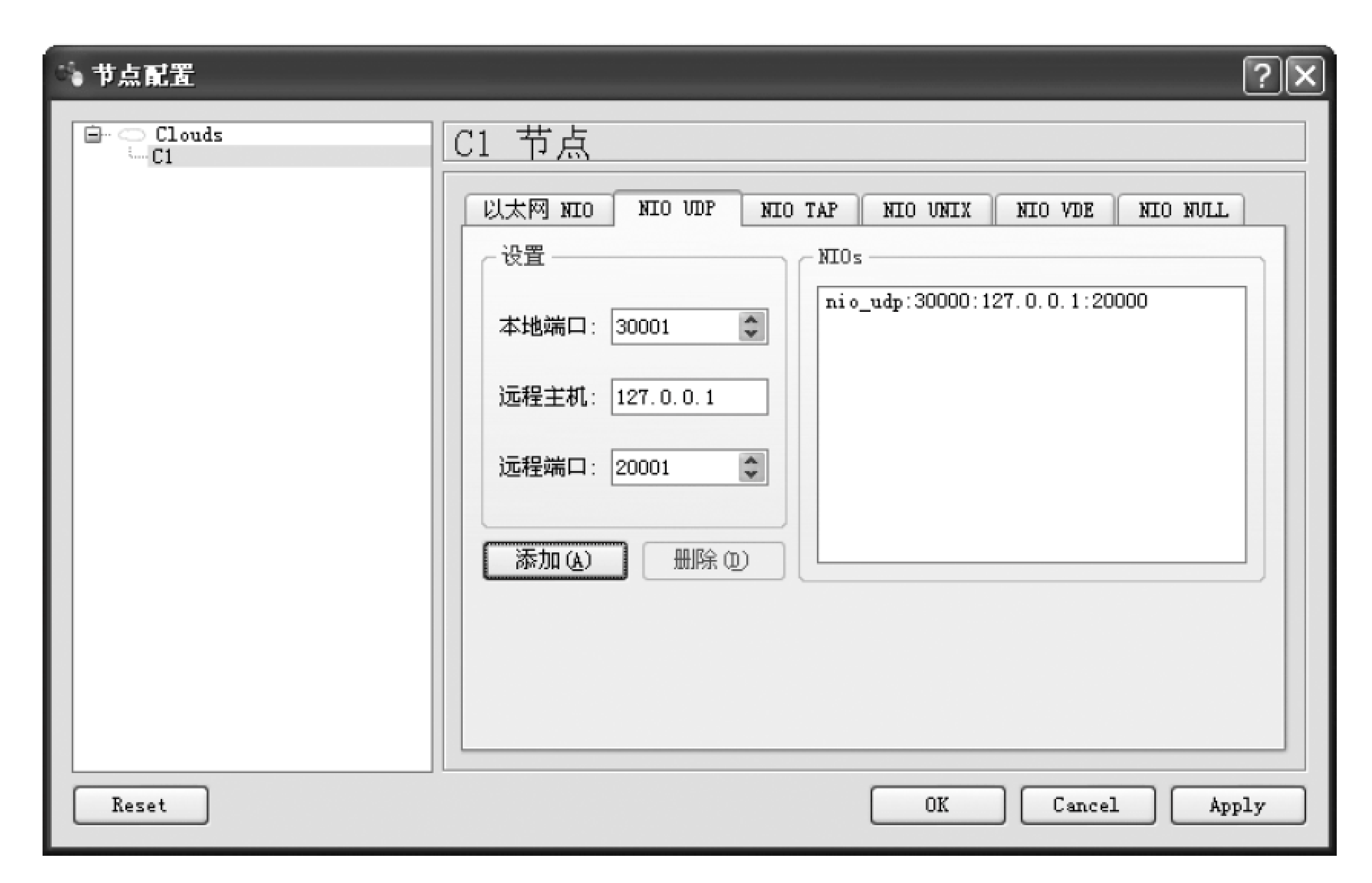


图 3-7-7　对 C1 进行配置

⑤ 对 C2 进行配置：右击 C2 图标，选择“配置”→NIO UDP，进行设置后，单击“添加”按钮后单击 OK 按钮，如图 3-7-8 所示。

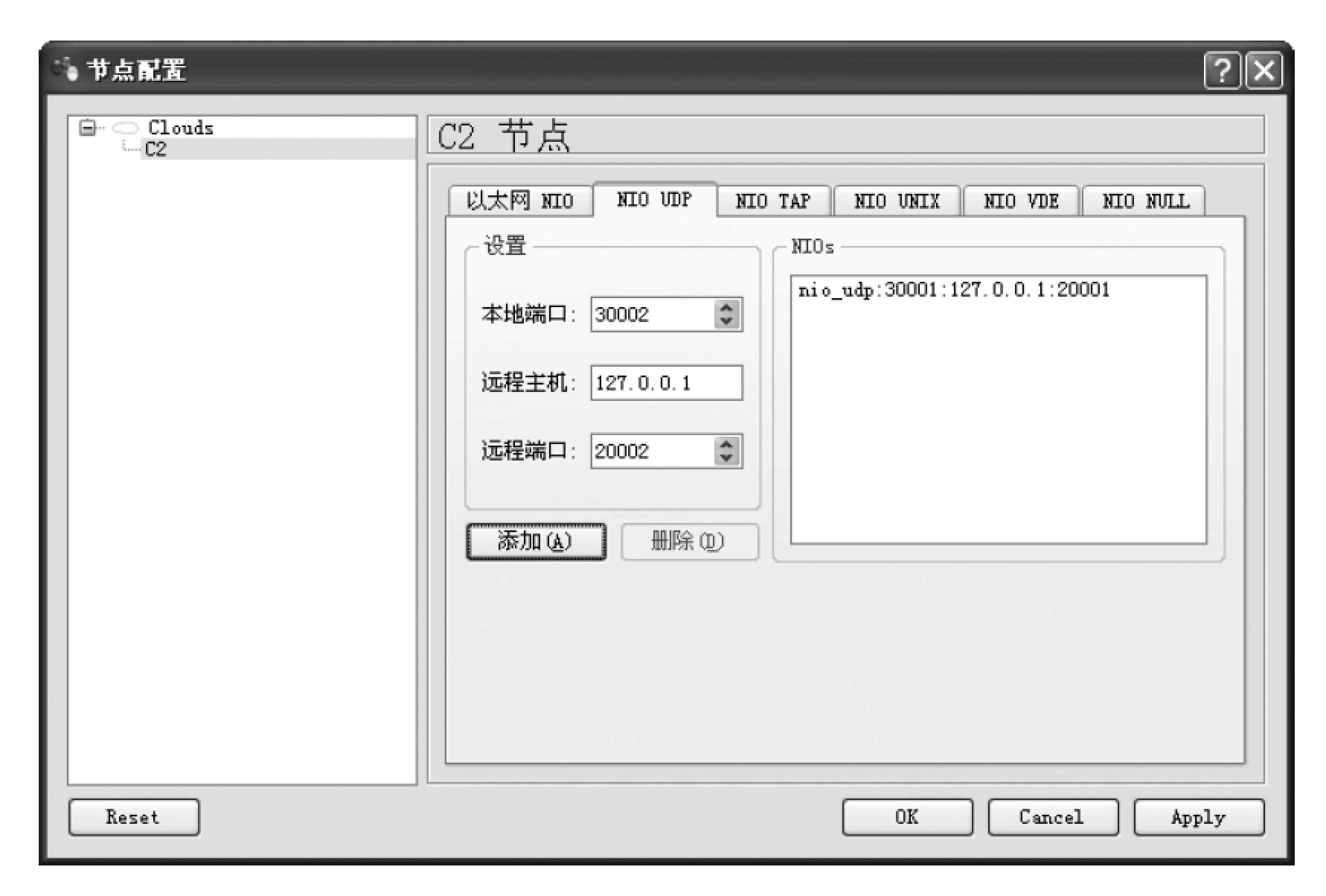


图 3-7-8 对 C2 进行配置

⑥ 对 C3 进行配置：右击 C3 图标，选择“配置”→NIO UDP，进行设置后，单击“添加”按钮后单击 OK 按钮，如图 3-7-9 所示。

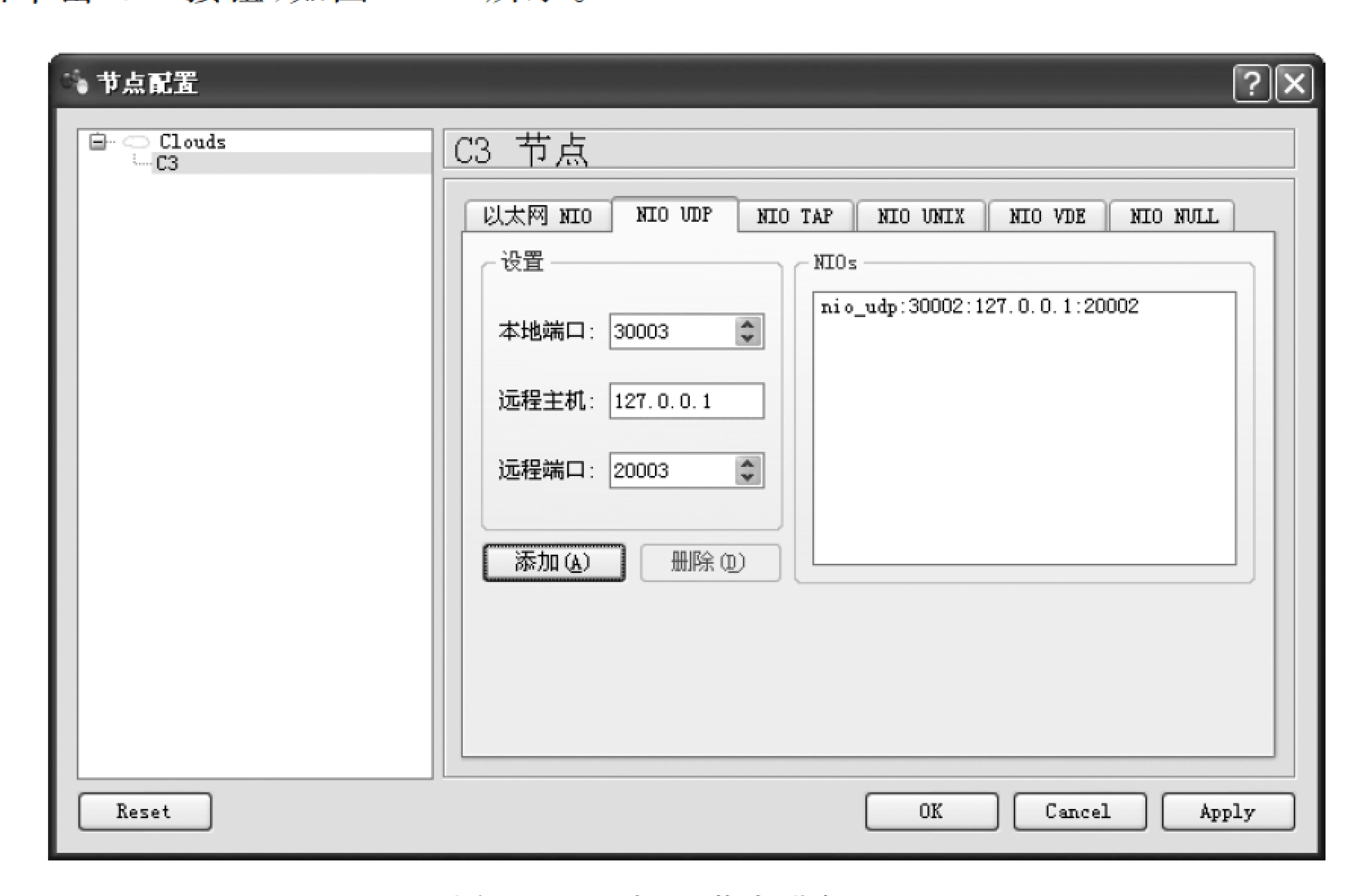


图 3-7-9 对 C3 节点进行配置

⑦ 对路由器 R1 的节点的配置如图 3-7-10 所示。

⑧ 对路由器 R2 的节点的配置如图 3-7-11 所示。

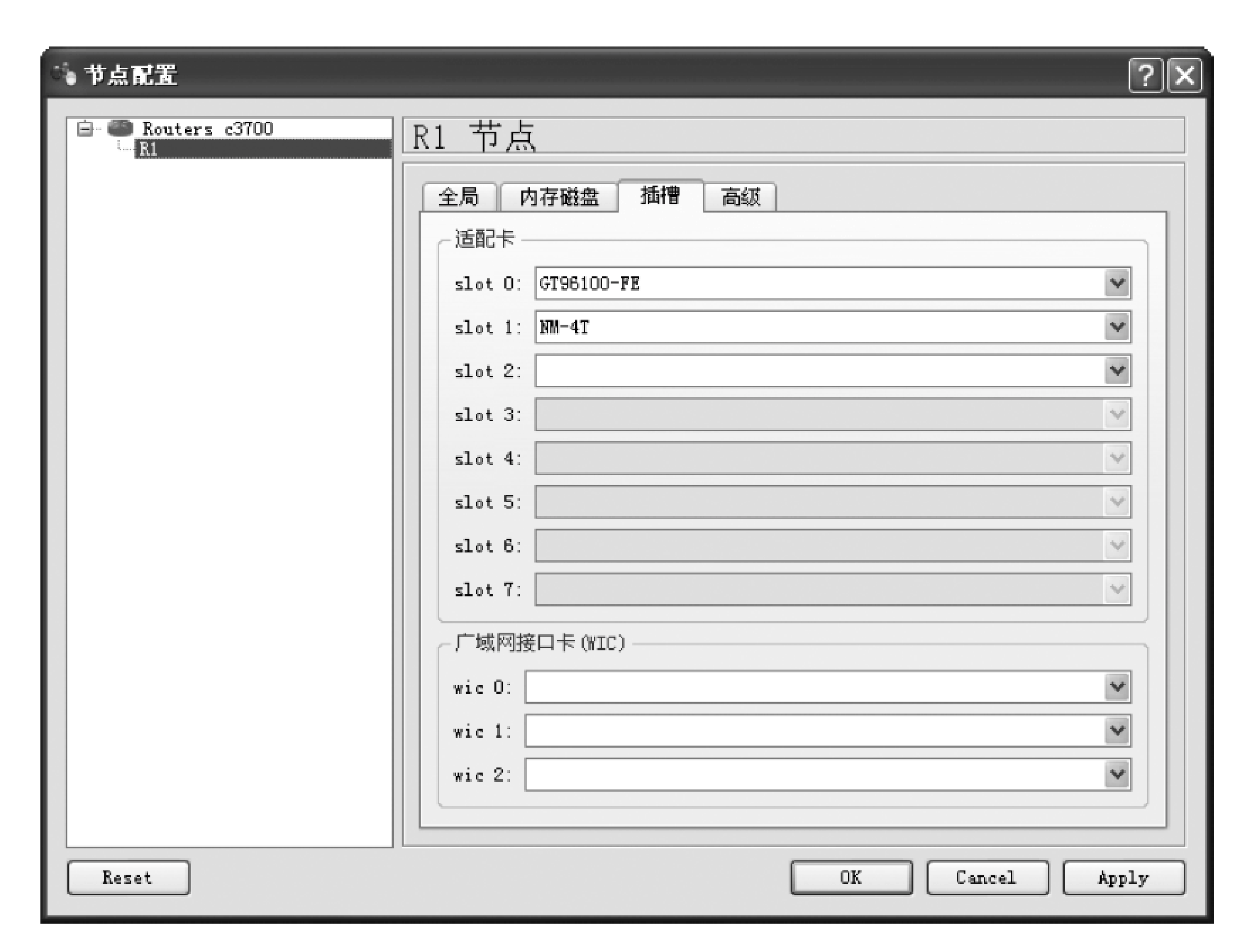


图 3-7-10　对 R1 节点进行配置

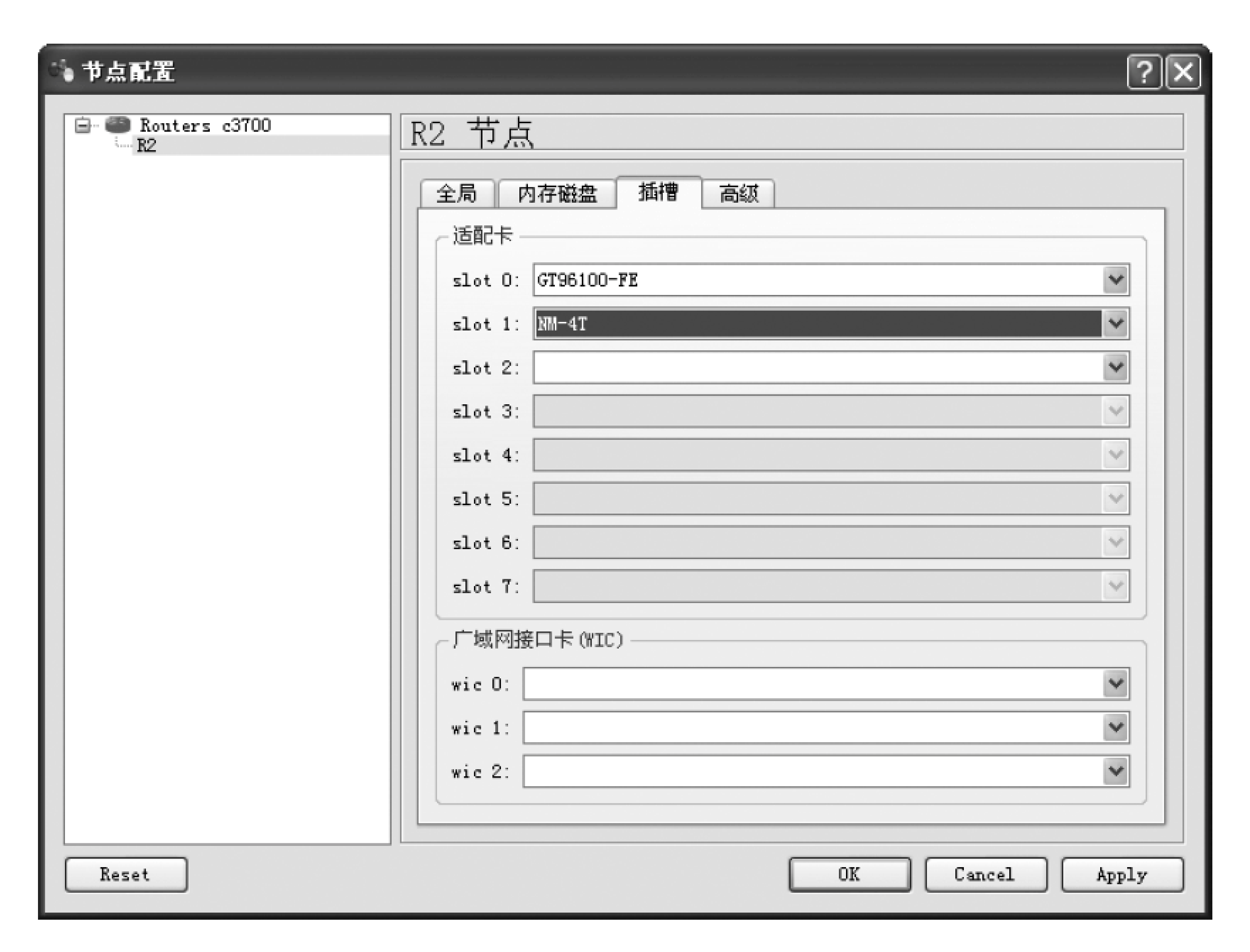


图 3-7-11　对 R2 进行配置

⑨ 对路由器 R3 的节点的配置如图 3-7-12 所示。

⑩ 在各设备间进行连线,生成节点,如图 3-7-13 所示。

⑪ 生成拓扑图,如图 3-7-14 所示。

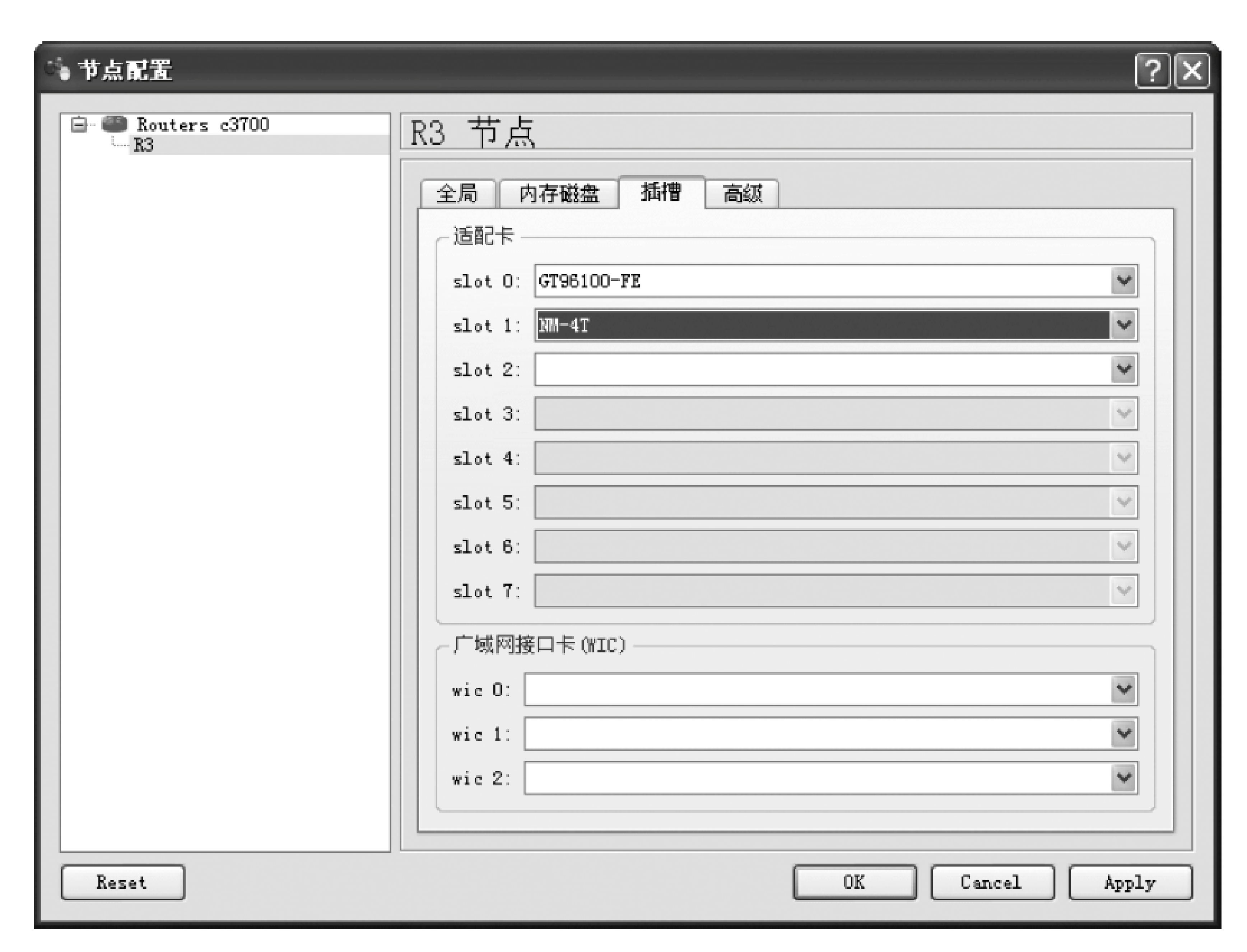


图 3-7-12　对 R3 节点进行配置

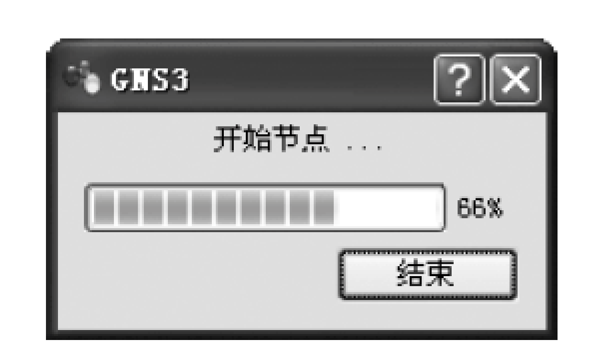


图 3-7-13　生成节点

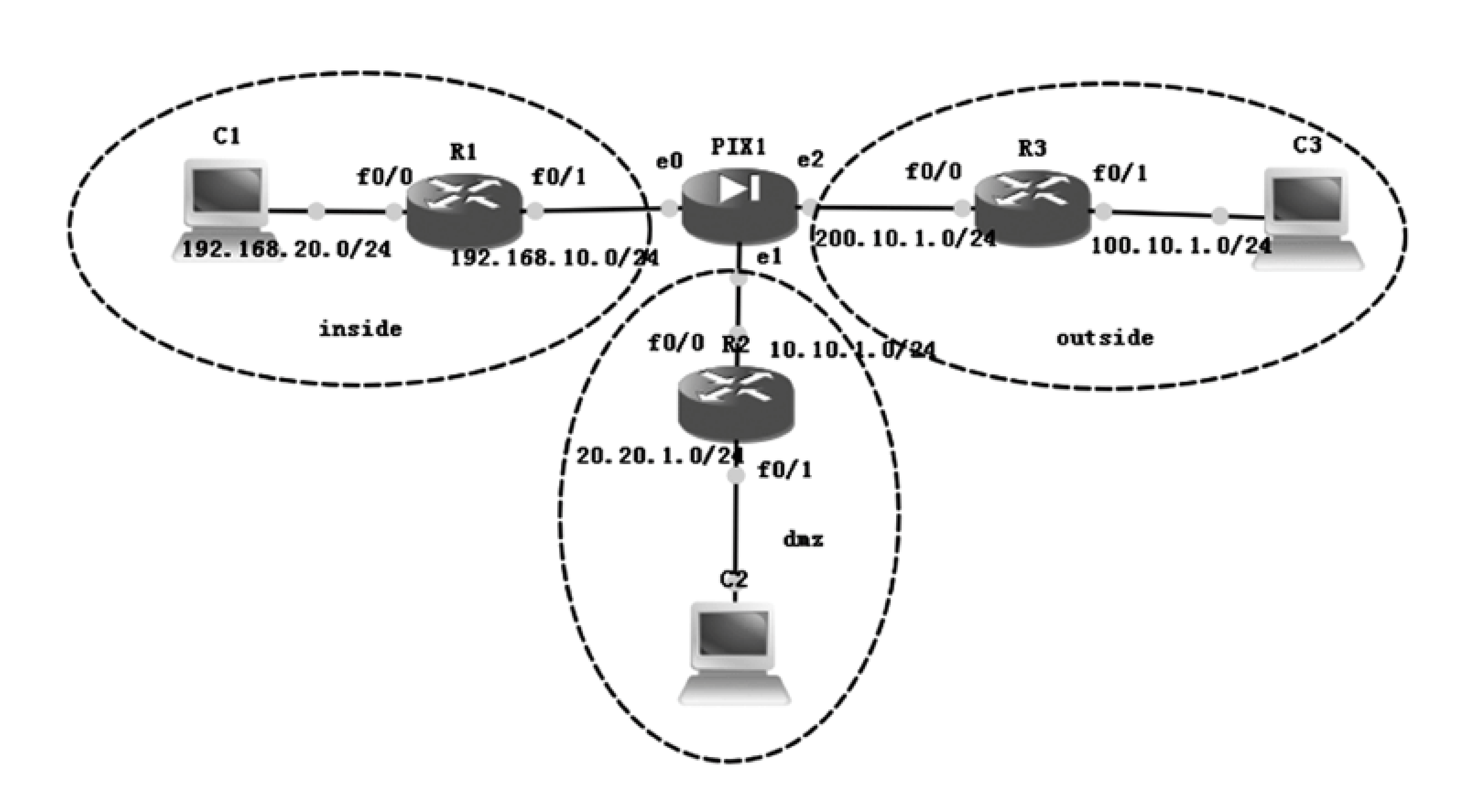


图 3-7-14　生成拓扑图

(3) 用防火墙划分内网、外网、DMZ 区域，配好接口 IP 地址以及安全级别。

① 在防火墙上为各个端口配置 IP 地址以及安全级别，安全级别默认为 outside，即 0，一般习惯默认 dmz 安全级别为 50，默认 inside 安全级别为 100，如图 3-7-15 所示。

```
pixfirewall> en
Password:
pixfirewall# conf t
pixfirewall(config)# nameif inside
                             ^
ERROR: % Invalid input detected at '^' marker.
pixfirewall(config)# int e0
pixfirewall(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
pixfirewall(config-if)# security-level 100
pixfirewall(config-if)# ip add 192.168.10.1 255.255.255.0
pixfirewall(config-if)# no shut
pixfirewall(config-if)# exit
pixfirewall(config)# int e1
pixfirewall(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
pixfirewall(config-if)# security-level 50
pixfirewall(config-if)# ip add 10.10.1.1 255.255.255.0
pixfirewall(config-if)# no shut
pixfirewall(config-if)# exit
pixfirewall(config)# int e2
pixfirewall(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
pixfirewall(config-if)# security-level 0
pixfirewall(config-if)# ip add 200.10.1.1 255.255.255.0
pixfirewall(config-if)# no shut
pixfirewall(config-if)# exit
```

图 3-7-15 配置 IP

② 配置 IP 地址之后，注意 ping 一下直连，结果如图 3-7-16 所示。

```
pixfirewall# ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/20/50 ms
pixfirewall# ping 10.10.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/30/60 ms
pixfirewall# ping 200.10.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/16/40 ms
```

图 3-7-16 ping IP

③ 配置路由器 R1 的 f0/1 端口的 IP 地址为 192.168.10.2，配置 f0/0 端口的 IP 地址为 192.168.20.2，如图 3-7-17 所示。

```
*Mar  1 00:14:18.839: %SYS-5-CONFIG_I: Configured from console by console
Router>
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip add 192.168.20.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int f0/1
Router(config-if)#ip add 192.168.10.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#end
Router#
*Mar  1 00:15:45.743: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:15:46.339: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:15:47.339: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

图 3-7-17 配置路由器

④ 配置路由器 R2 的 f0/0 端口的 IP 地址为 10.10.1.2,配置 f0/1 端口的 IP 地址为 20.20.1.2,如图 3-7-18 所示。

```
Router#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int f0/0
R2(config-if)#ip add 10.10.1.2 255.255.255.0[~
                                            ^
% Invalid input detected at '^' marker.

R2(config-if)#ip add 10.10.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#i
*Mar  1 00:19:46.315: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:19:47.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
% Incomplete command.

R2(config)#int f0/1
R2(config-if)#ip add 20.20.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
*Mar  1 00:20:09.767: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to upe
*Mar  1 00:20:10.767: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
% Ambiguous command:  "e"
R2(config)#exit
R2#wr
Building configuration...

*Mar  1 00:20:13.927: %SYS-5-CONFIG_I: Configured from console by console[OK]
```

图 3-7-18　配置 R2

⑤ 配置路由器 R3 的 f0/0 端口的 IP 地址为 200.10.1.2,配置 f0/1 端口的 IP 地址为 100.10.1.2,如图 3-7-19 所示。

```
Router(config)#hostname R3
R3(config)#int f0/0
R3(config-if)#ip add 200.10.1.2 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#int f0/0
*Mar  1 00:23:02.075: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:23:03.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config-if)#int f0/1
R3(config-if)#ip add 100.10.1.2 255.255.255.0
R3(config-if)#no shut
R3(config-if)#end
R3#wr
Building configuration...

*Mar  1 00:23:28.511: %SYS-5-CONFIG_I: Configured from console by console[OK]
R3#
R3#
*Mar  1 00:23:29.095: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:23:32.403: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

图 3-7-19　配置 R3

⑥ 允许 DMZ 区域的主机的 ICMP 协议的报文访问出去,将策略应用在 dmz 接口上,如图 3-7-20 所示。

```
pixfirewall# conf t
pixfirewall(config)# access-list dmz permit icmp any any
pixfirewall(config)#  access-group dmz in interface dmz
pixfirewall(config)# end
pixfirewall# wr
Building configuration...
Cryptochecksum: d54baada 45589982 c85d4817 22ef9dd4

1710 bytes copied in 1.300 secs (1710 bytes/sec)
[OK]
```

图 3-7-20　配置策略

⑦ 到 R1 上测试一下，ping 一下 dmz 主机 10.10.1.2，图 3-7-21 中显示并没有 ping 通，此时应该在各个路由器上添加动态路由 RIP。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#ping 10.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#
Router#ping 192.168.10.1

Type escape sequence to abort.
```

图 3-7-21　在 R1 测试

⑧ 在 R1 上添加动态路由 RIP，如图 3-7-22 所示。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/51/128 ms
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.20.0
Router(config-router)#end
Router#pin
*Mar  1 00:30:13.403: %SYS-5-CONFIG_I: Configured from console by consoleg
Protocol [ip]:
Target IP address:
% Bad IP address
```

图 3-7-22　R1 添加动态路由

⑨ 在 R2 上添加动态路由 RIP，如图 3-7-23 和图 3-7-24 所示。

```
R2>
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.10.1.0
R2(config-router)#network 20.20.1.0
R2(config-router)#end
R2#wr
Building configuration...
[OK]
R2#
*Mar  1 00:33:23.559: %SYS-5-CONFIG_I: Configured from console by console
```

图 3-7-23　R2 添加动态路由

⑩ 在 R3 上添加动态路由 RIP，如图 3-7-25 所示。

⑪ 在各个路由器上添加完动态路由 RIP 后，到 R1 上测试一下，ping 一下 dmz 主机 10.10.1.2，图 3-7-26 中显示 ping 通，说明 R1 和 DMZ 主机之间已经建立了通信。

⑫ 同样为了允许外网接口 ICMP 的回包，需要在防火墙上进行如图 3-7-27 所示的配置。

⑬ 到 R1 上测试一下，ping 一下 outside 主机 200.10.1.2，图 3-7-28 中显示 ping 通，说明 R1 和 outside 主机之间已经建立了通信。

```
R3(config-if)#end
R3#wr
Building configuration...

*Mar  1 00:23:28.511: %SYS-5-CONFIG_I: Configured from console by console[OK]
R3#
R3#
*Mar  1 00:23:29.095: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:23:32.403: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 200.10.1.0
R3(config-router)#network 100.10.1.0
R3(config-router)#
R3(config-router)#end
R3#wr
Building configuration...
[OK]
R3#
```

图 3-7-24　添加动态路由

```
R3(config-if)#end
R3#wr
Building configuration...

*Mar  1 00:23:28.511: %SYS-5-CONFIG_I: Configured from console by console[OK]
R3#
R3#
*Mar  1 00:23:29.095: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:23:32.403: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 200.10.1.0
R3(config-router)#network 100.10.1.0
R3(config-router)#
R3(config-router)#end
R3#wr
Building configuration...
[OK]
R3#
```

图 3-7-25　R3 添加动态路由

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/40/60 ms
Router#ping 10.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/28/76 ms
Router#ping 10.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/64 ms
```

图 3-7-26　R1 测试

```
pixfirewall# conf t
pixfirewall(config)# access-list outside permit icmp any any echo-reply
WARNING: <outside> found duplicate element
pixfirewall(config)# access-group outside in interface outside
pixfirewall(config)# end
pixfirewall# wr
Building configuration...
Cryptochecksum: 5ec67d4e bea4dcb0 dc68e02c e99dc7f1

1888 bytes copied in 1.430 secs (1888 bytes/sec)
[OK]
```

图 3-7-27　防火墙配置

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#END
R1#PIN
*Mar  1 00:53:56.743: %SYS-5-CONFIG_I: Configured from console by consoleG
Protocol [ip]:
Target IP address:
% Bad IP address
R1#ping 200.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/42/96 ms
```

图 3-7-28　ping outside 主机

(4) 防火墙静态路由配置。

① 在防火墙上配置静态路由,如图 3-7-29 所示。

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/16/40 ms
pixfirewall# conf t
pixfirewall(config)# route dmz 20.20.1.0 255.255.255.0 10.10.1.2
pixfirewall(config)#  route dmz 20.20.1.0 255.255.255.0 10.10.1.2
pixfirewall(config)# end
pixfirewall# conf t
pixfirewall(config)#  route dmz 20.20.1.0 255.255.255.0 10.10.1.2
```

图 3-7-29　配置静态路由

dmz:表示接口名称。

20.20.1.0 255.255.255.0:表示目的网段。

10.10.1.2:表示下个路由器的 IP 地址,也就是下一跳地址。

1:[metric]路由花费。默认值是 1。route dmz 20.20.1.0 255.255.255.0 10.10.1.2。

② 在 R1 上测试一下,ping 一下 20.20.1.2,图 3-7-30 显示 ping 通了,表示静态路由配置成功。

```
R1>en
R1#ping 20.20.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/62/216 ms
```

图 3-7-30　静态路由配置成功

(5) 防火墙上的 NAT 配置,实现内网访问外网。

① nat 命令的配置语法:

```
nat(if_name)nat_idlocal_ip[netmark]
```

其中:

(if_name):表示接口名称,一般为 inside。

nat_id:表示地址池,由 global 命令定义。

local_ip:表示内网的 IP 地址。对于 0.0.0.0 表示内网所有主机。

[netmark]:表示内网 IP 地址的子网掩码。

② Global 命令的配置语法,Global 指定公网地址范围,定义地址池:

global (if_name) nat_id ip_address-ip_address [netmarkglobal_mask]

其中：

(if_name)：表示外网接口名称，一般为 outside。

nat_id：建立的地址池标识(nat 要引用)。

ip_address-ip_address：表示一段 IP 地址范围。

[netmarkglobal_mask]：表示全局 IP 地址的网络掩码。

③ 在防火墙上的配置如图 3-7-31 所示。

```
pixfirewall(config)# globle (outside) 1 interface
                                   ^
ERROR: % Invalid input detected at '^' marker.
pixfirewall(config)# globle (outside) 1 interface
                                   ^
ERROR: % Invalid input detected at '^' marker.
pixfirewall(config)# end
pixfirewall# conf t
pixfirewall(config)# nat (inside) 1 0 0
Duplicate NAT entry
pixfirewall(config)# global (outside) 1 interface
INFO: outside interface address added to PAT pool
```

图 3-7-31　防火墙配置

④ 在 R1 上测试一下，ping 一下外网主机 200.10.1.2，图 3-7-32 显示 ping 通了，表示实现了内网访问外网。

```
[OK]
R1#ping
Protocol [ip]:
Target IP address:
% Bad IP address
R1#ping 200.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/33/76 ms
```

图 3-7-32　ping 外网

(6) 实现外网访问 DMZ 区域的 Web 服务器，配置防火墙的反向 NAT。

① 配置命令分析：

允许外网访问 dmz 的 80 端口的配置命令为：

access-list 100 permit tcp any host 202.101.1.1 eq 80

将 DMZ 区域的 Web 发布到公网上的配置命令为：

access-group 100 in interface outside

static (inside,outside) tcp interface www 10.1.1.2 www network 255.255.255.255

② 在防火墙上进行配置，如图 3-7-33 所示。

```
ERROR: % Invalid Hostname
pixfirewall(config)# access-list 100 permit tcp any host 200.10.1.1 eq 80
WARNING: <100> found duplicate element
pixfirewall(config)# access-group 100 in interface outside
pixfirewall(config)# S interface www 10.10.1.2 www network 255.255.255.255
```

图 3-7-33　防火墙配置

(7) 防火墙流量限制配置。

① 流量限制为512k/s,配置命令如下:

```
pixfirewall(config)#priority-queue outside
pixfirewall(config-priority-queue)#queue-limit 512
```

② 在防火墙上进行配置,如图3-7-34所示。

```
pixfirewall(config)# priority-queue outside
pixfirewall(config-priority-queue)# queue-limit 512
```

图3-7-34 防火墙配置

3.7.8 实验思考

硬件防火墙与软件防火墙之间的区别是什么?

3.8 入侵检测

3.8.1 实验类型

综合型,4学时,必选实验。

3.8.2 实验目的

入侵检测系统通过检查操作系统的审计数据或网络数据包信息,检测系统中违背安全策略或危及系统安全的行为或活动,从而保护信息系统。通过实验,使学生认识入侵检测的重要作用,了解入侵检测系统的类型、工作原理和常用产品,掌握网络入侵检测系统的规划、配置、使用方法。

3.8.3 题目描述

在Windows操作系统下配置并使用Snort进行入侵检测。

3.8.4 实验要求

能够配置Snort入侵检测系统,利用Snort规则库进行入侵检测。

3.8.5 相关知识

Snort是一个强大的轻量级的网络入侵检测系统。它具有实时数据流量分析和日志

IP 网络数据包的能力，能够进行协议分析，对内容进行搜索/匹配。它能够检测各种不同的攻击方式，对攻击进行实时报警，还具有很好的扩展性和可移植性。此外，这个软件遵循通用公共许可证(GPL)，所以只要遵守 GPL 的任何组织和个人都可以自由使用。

(1) Snort 是一个轻量级的入侵检测系统。

Snort 虽然功能强大，但是其代码极为简洁、短小，其源代码压缩包只有大约 110KB。

(2) Snort 的可移植性很好。

Snort 的跨平台性能极佳，目前已经支持 Linux、Solaris、BSD、IRIX、HP-UX 和 WinY2K 等系统。

(3) Snort 的功能非常强大。

Snort 具有实时流量分析和日志 IP 网络数据包的功能，能够快速检测网络攻击，及时发出报警。Snort 的报警机制很丰富，例如 syslog、用户指定的文件、一个 UNIX 套接字，还能使用 SAMBA 协议向 Windows 客户程序发出 WinPopup 消息。利用 XML 插件，Snort 可以使用简单网络标记语言(Simple Network Markup Language，SNML)把日志存储到一个文件中或者适时报警。

Snort 能够进行协议分析、内容搜索/匹配。现在 Snort 能够分析的协议有 TCP、UDP 和 ICMP，将来可能提供对 ARP、ICRP、GRE、OSPF、RIP、IPX 等协议的支持。它能够检测多种方式的攻击和探测，例如缓冲区溢出、秘密端口扫描、CGI 攻击、SMB 探测、探测操作系统指纹特征的企图等。

Snort 的日志格式既可以是 tcpdump 式的二进制格式，也可以解码成 ASCII 字符形式，更加便于用户尤其是新手检查。使用数据库输出插件，Snort 可以把日志记入数据库，当前支持的数据库包括 Postgresql、MySQL、任何 unixODBC 数据库，还有 Oracle(对 Oracle 的支持目前处于测试阶段)。

使用 TCP 流插件(tcpstream)，Snort 可以对 TCP 包进行重组。Snort 能够对 IP 包的内容进行匹配，但是对于 TCP 攻击，如果攻击者使用一个程序，每次发送只有一个字节的 TCP 包，完全可以避开 Snort 的模式匹配。而被攻击的主机的 TCP 协议栈会重组这些数据，将其送给在目标端口上监听的进程，从而使攻击包逃过 Snort 的监视。使用 TCP 流插件，可以对 TCP 包进行缓冲，然后进行匹配，使 Snort 具备对付上面这种攻击的能力。

使用 spade(Statistical Packet Anomaly Detection Engine)插件，Snort 能够报告非正常的可疑包，从而对端口扫描进行有效的检测。

Snort 还有很强的系统防护能力。使用 FlexResp 功能，Snort 能够主动断开恶意连接。

(4) 扩展性能较好，对于新的攻击威胁反应迅速。

作为一个轻量级的网络入侵检测系统，Snort 有足够的扩展能力。它使用一种简单的规则描述语言。最基本的规则只包含 4 个域：处理动作、协议、方向和注意的端口。例如 log tcp any any→10.1.1.0/24 79。还有一些功能选项可以组合使用，实现更为复杂的功能。

Snort 支持插件，可以使用具有特定功能的报告、检测子系统插件对其功能进行扩展。Snort 当前支持的插件包括数据库日志输出插件、碎数据包检测插件、端口扫描检测插件、HTTP URI normalization 插件和 XML 插件等。

Snort 的规则语言非常简单，能够对新的网络攻击做出很快的反应。发现新的攻击后，可以很快根据 Bugtraq 邮件列表找出特征码，写出检测规则。因为其规则语言简单，所以很容易上手，节省人员的培训费用。

(5) 遵循公共通用许可证 GPL。

Snort 遵循 GPL，所以任何企业、个人和组织都可以免费使用它作为自己的 NIDS。

3.8.6 实验设备

硬件环境：主流配置 PC 3 台

操作系统：Windows XP 工具手段：开源的工具软件及其支持附件：

(1) WinPcap_3_0.exe：Windows 下捕获网络数据包的驱动程序库，http://www.winpcap.org/。

(2) Snort_2_4_5_Installer.exe：将其捕获的数据发送至数据库，http://www.snort.org/。

(3) appserv-win32-2.4.1.exe：可快速建立 Apache/PHP/MySQL 环境，http://www.appservnetwork.com/? modules=&applang=tw。

(4) acid-0.9.6b23.tar.gz：PHP 网页模式的入侵侦测数据库分析控制台，http://www.cert.org/kb/acid/。

(5) adodb461.zip：PHP 数据库链接库，http://adodb.sourceforge.net/。

(6) jpgraph-1.17.tar.gz：Object-Oriented 图形链接库 For PHP，http://www.aditus.nu/jpgraph/。

3.8.7 实验步骤

(1) 检查使用的计算机的 Windows 操作系统是否安装 IIS。

如果安装，需要卸载。方法如下：打开“控制面板”→“增加或删除程序”，选择“增加或删除 Windows 组件”。如果 Internet 信息服务(IIS)的选项框处于选中状态，如图 3-8-1 所示，则取消对“Internet 信息服务(IIS)”选项框的选中，单击“下一步”按钮，根据向导进行 IIS 的卸载。卸载完成后，出现完成画面，如图 3-8-2 所示，单击“完成”按钮退出卸载，然后退出“增加或删除程序”和“控制面板”，准备进行 Apache/PHP/MySQL 环境的安装。

(2) 安装 AppServ。

① 运行 appserv-win32-2.4.1.exe，根据安装向导提示进行安装，如图 3-8-3 所示。

② 安装过程中需输入 Apache HTTP Server Information，根据实际需求填写，如图 3-8-4所示。



图 3-8-1 “Windows 组件向导”界面



图 3-8-2 完成“Windows 组件向导”界面

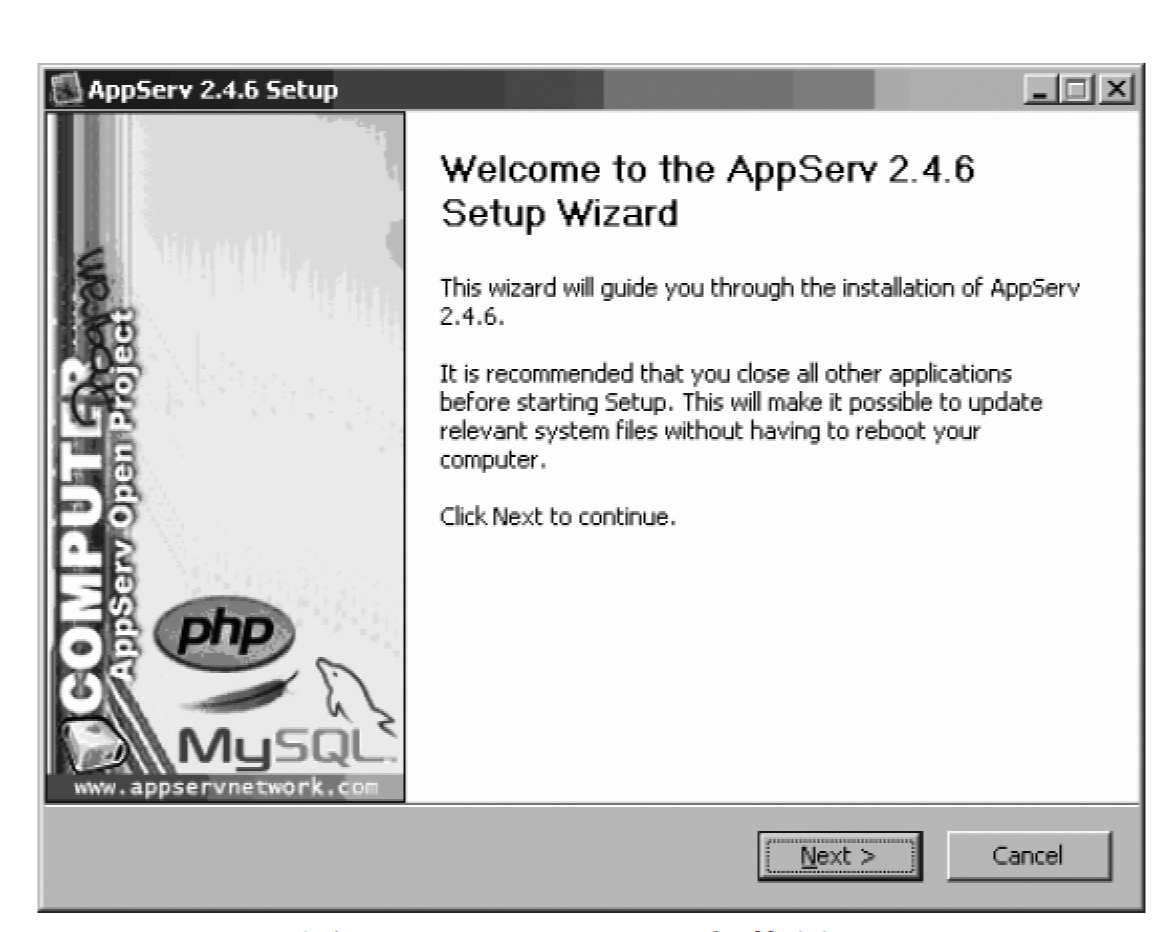


图 3-8-3 AppServ 安装界面

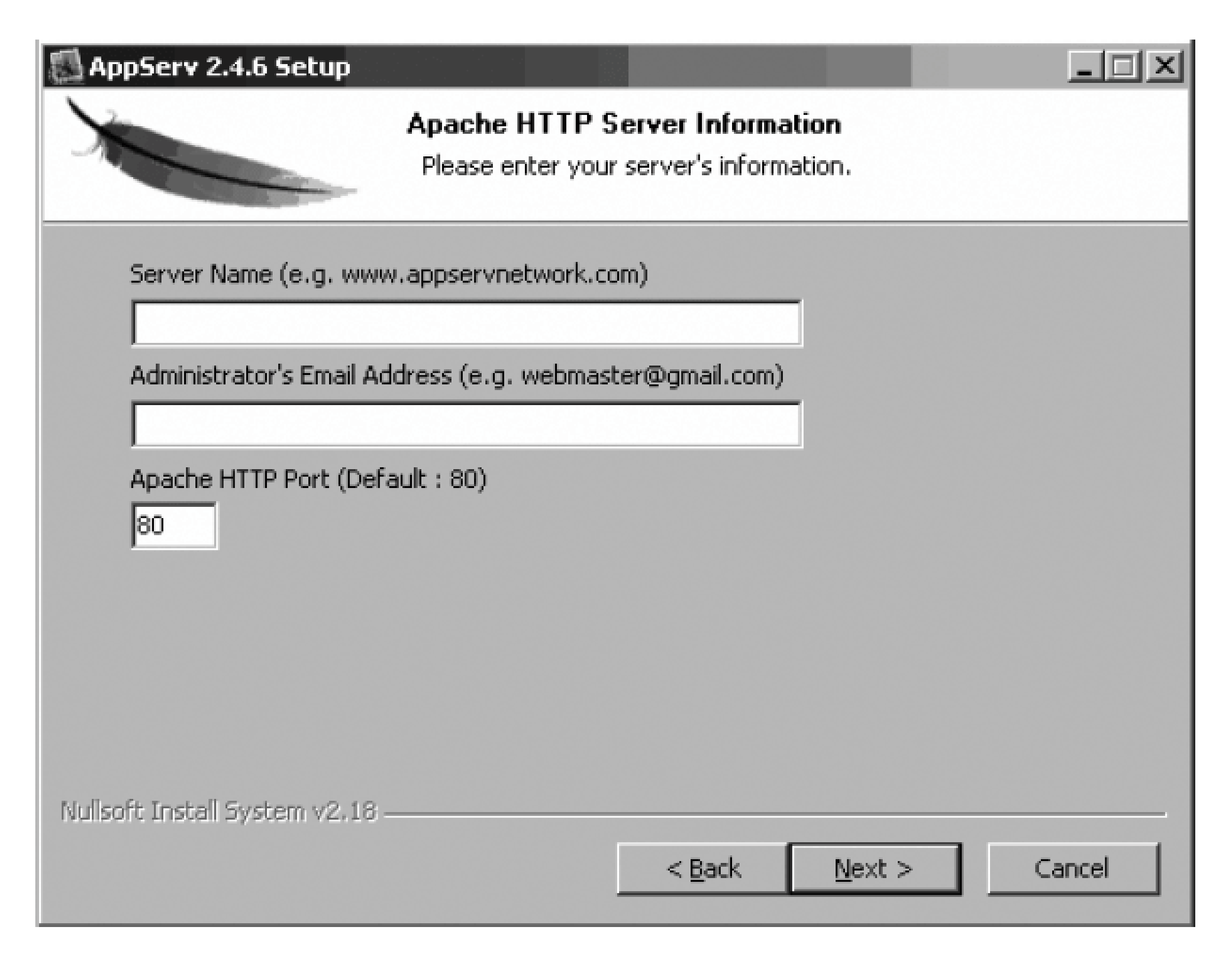


图 3-8-4　AppServ 输入 Apache HTTP server Information 界面

③ 安装过程中需输入 MySQL 中的 Root 用户密码，如图 3-8-5 所示。本实例以填写 123456 为例，后续关于该用户登录，均采用该密码。

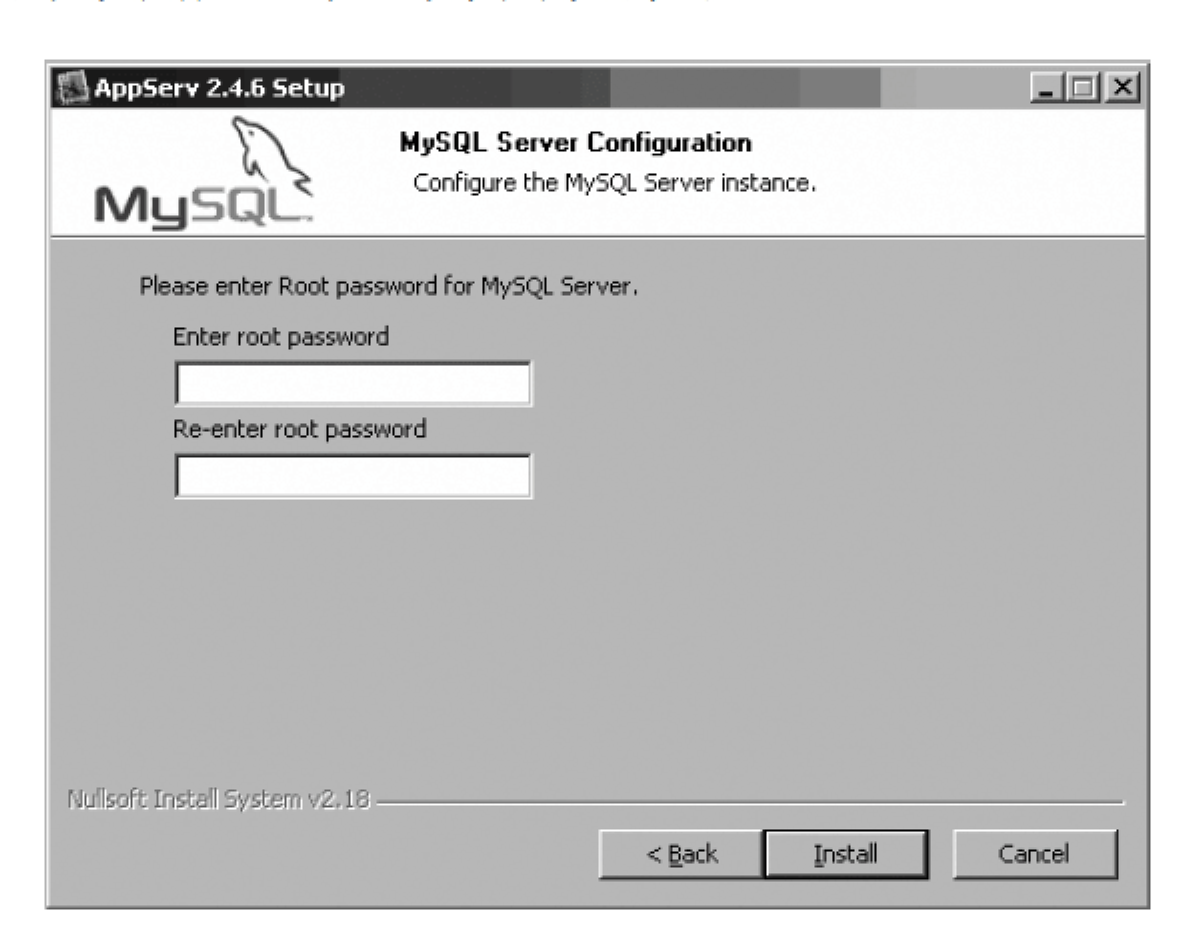


图 3-8-5　AppServ 输入 MySQL Server Configuration 界面

④ 在安装过程中若有防火墙予以拦截，应选择允许通过该服务，直至安装结束。安装结束后可以选中 Start Apache、Start MySQL 两个选项，如图 3-8-6 所示。

(3) 打开 Apache Monitor。

操作：打开"开始"→"所有程序"→AppServ→Control Server by Service→Apache Monitor，即可在运行框中看到 Apache 的运行图标了，如图 3-8-7 所示。

(4) 检测安装是否成功。

打开 IE 浏览器，输入 http://127.0.0.1/，成功安装出现图 3-8-8 所示界面。

(5) 登录 MySQL 数据库。

① 打开 IE 浏览器，输入 http://127.0.0.1/，单击 phpMyAdmin Database Manager

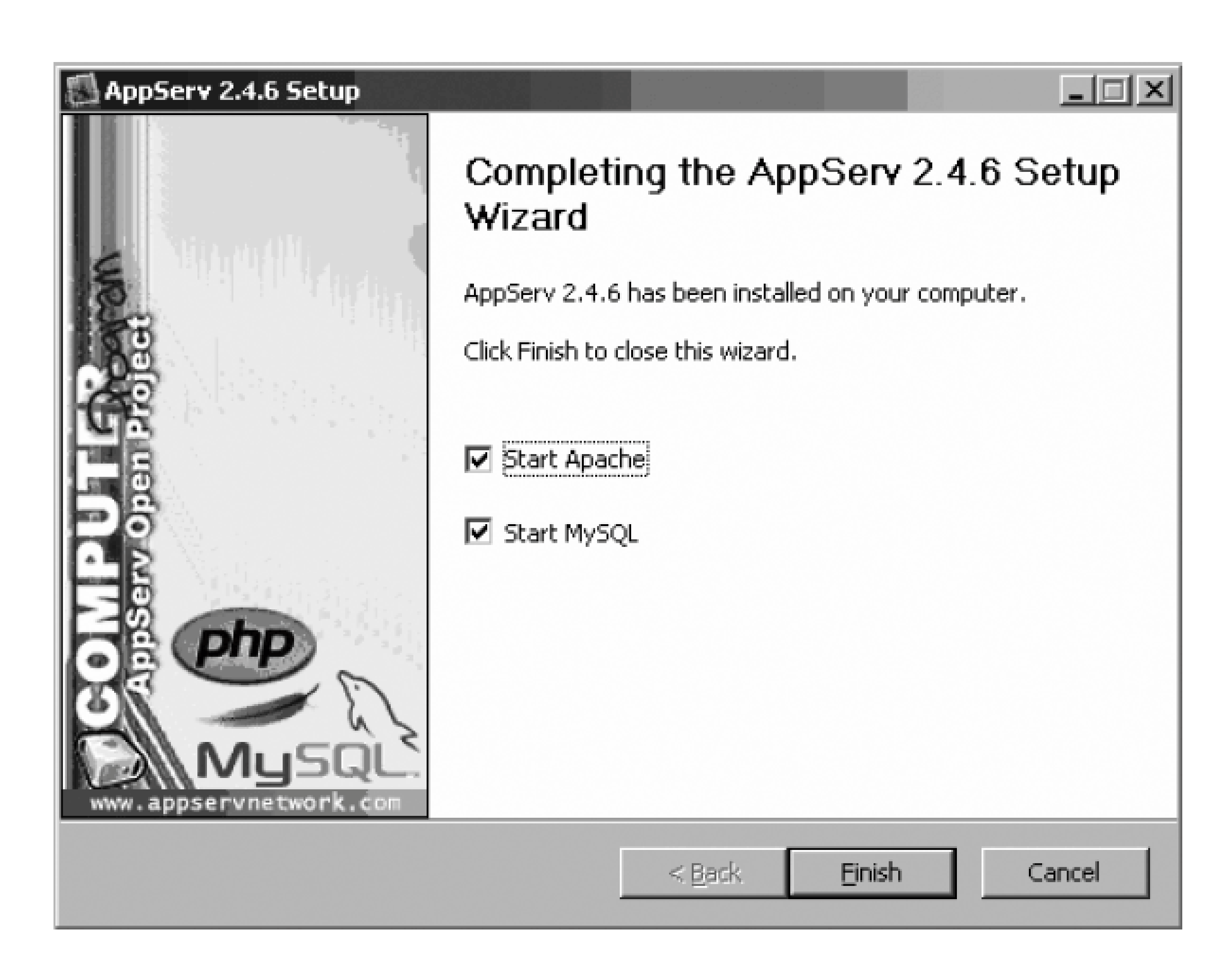


图 3-8-6　AppServ 安装结束界面

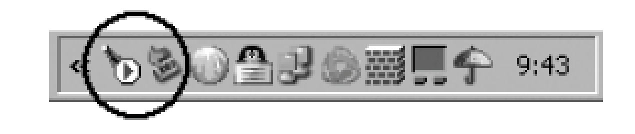


图 3-8-7　Apache Monitor 运行图标

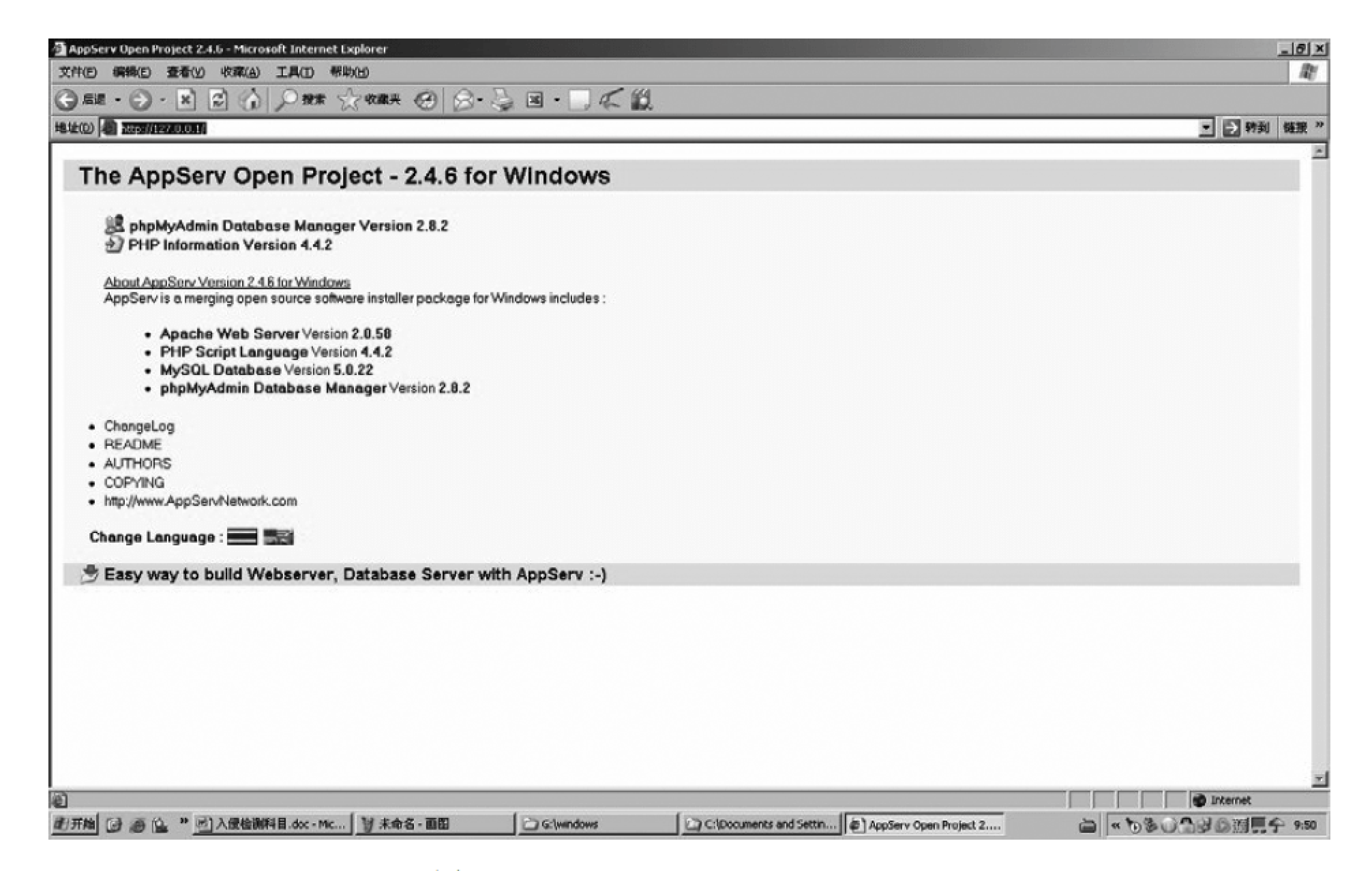


图 3-8-8　The AppServ Open Project

Version 2.8.2 出现登录对话框。"用户名"输入"root"，"密码"输入"123456"(安装时输入的 MySQL root 用户密码)，如图 3-8-9 所示。

② 单击"确认"按钮即可进入 phpMyAdmin，界面如图 3-8-10 所示。

(6) 检查 allow_call_time_pass_reference 设置。

打开 C:\Windows(Win 2000 下为 C:\winnt)NT 开启 php.ini 这个档案，寻找 allow_call_time_pass_reference 查看其设置，若 allow_call_time_pass_reference=Off 字符串，将它更改为 allow_call_time_pass_reference=On 后，存档离开。若需要修改，则双击右下角的 Apache Monitor，按下 Restart 按钮重新加载 php.ini，如图 3-8-11 所示。



图 3-8-9　MySQL 登录信息对话框



图 3-8-10　phpMyAdmin

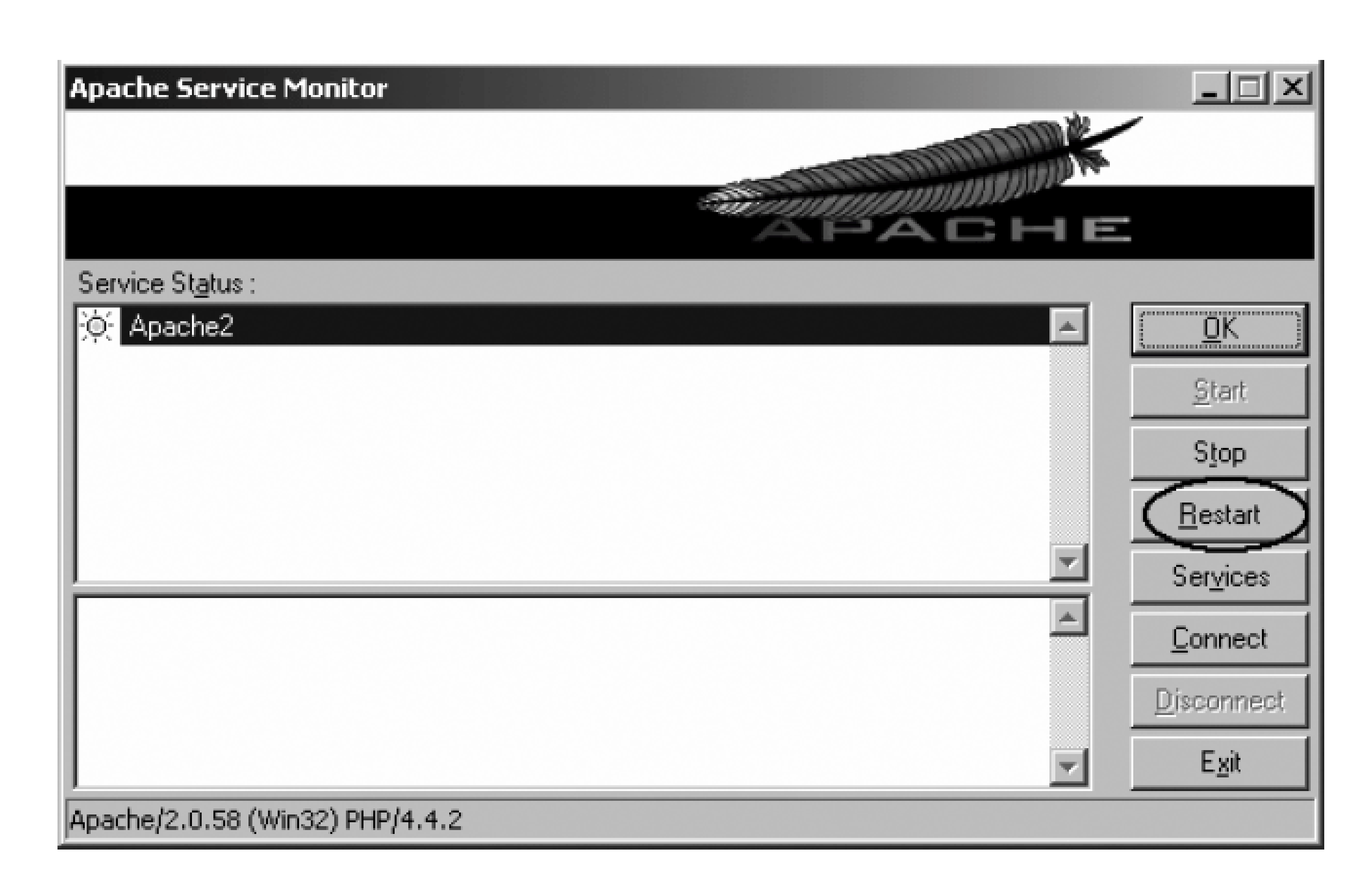


图 3-8-11　Apache Service Monitor

（7）测试 Apache 安装是否正确。

打开 IE，输入 http://192.168.1.16，出现图 3-8-12 所示内容。

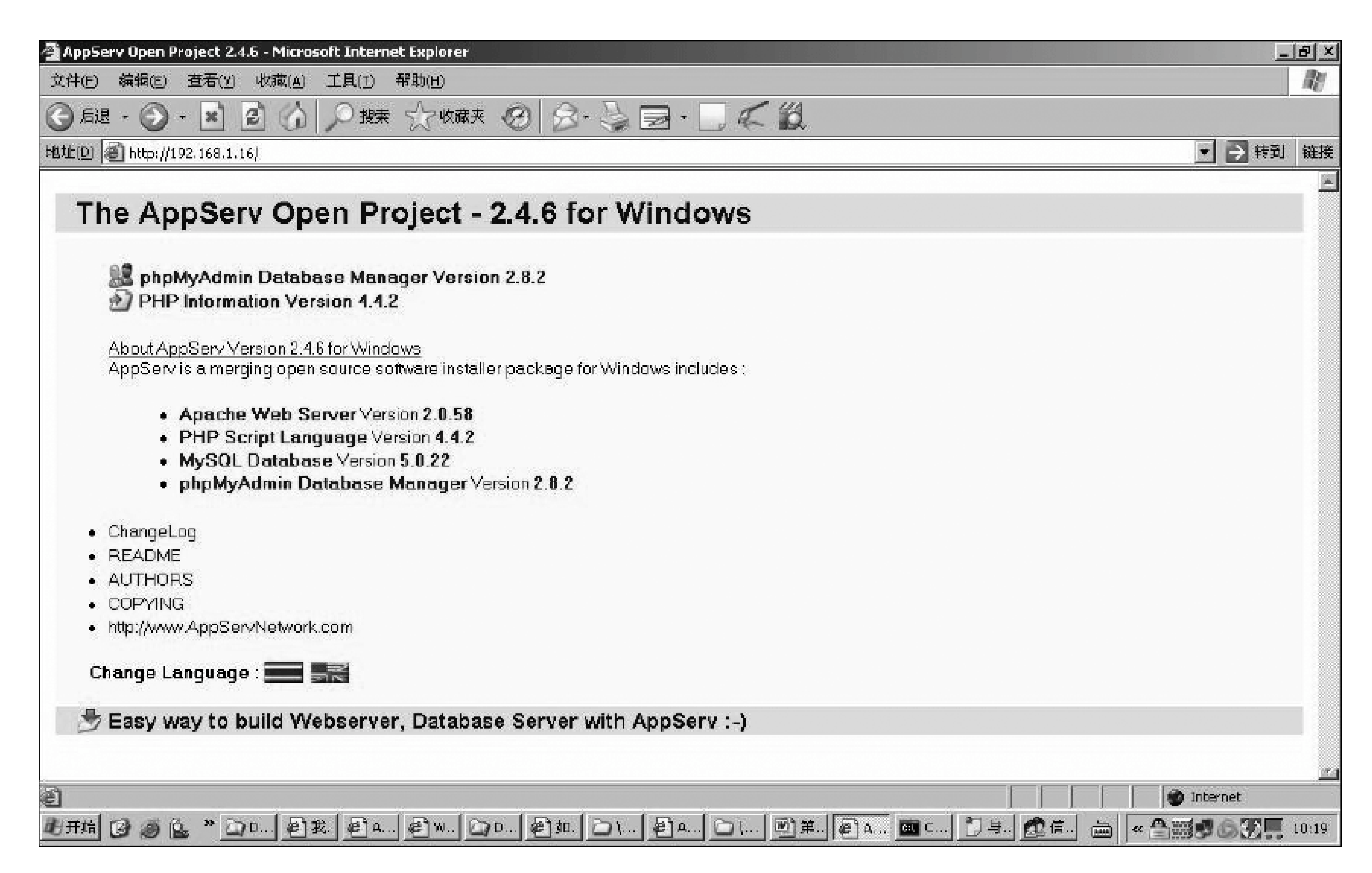


图 3-8-12　The AppServ Open Project

（8）在 MySQL 中建立 Snort 数据库存储 Snort 系统的信息方法如下：

① 首先登录 phpMyAdmin，然后单击数据库，进入 MySQL 数据库，如图 3-8-13 所示。



图 3-8-13　phpMyAdmin

② 输入数据库名 Snort 后单击“创建”按钮，创建 Snort 数据库，如图 3-8-14 所示。

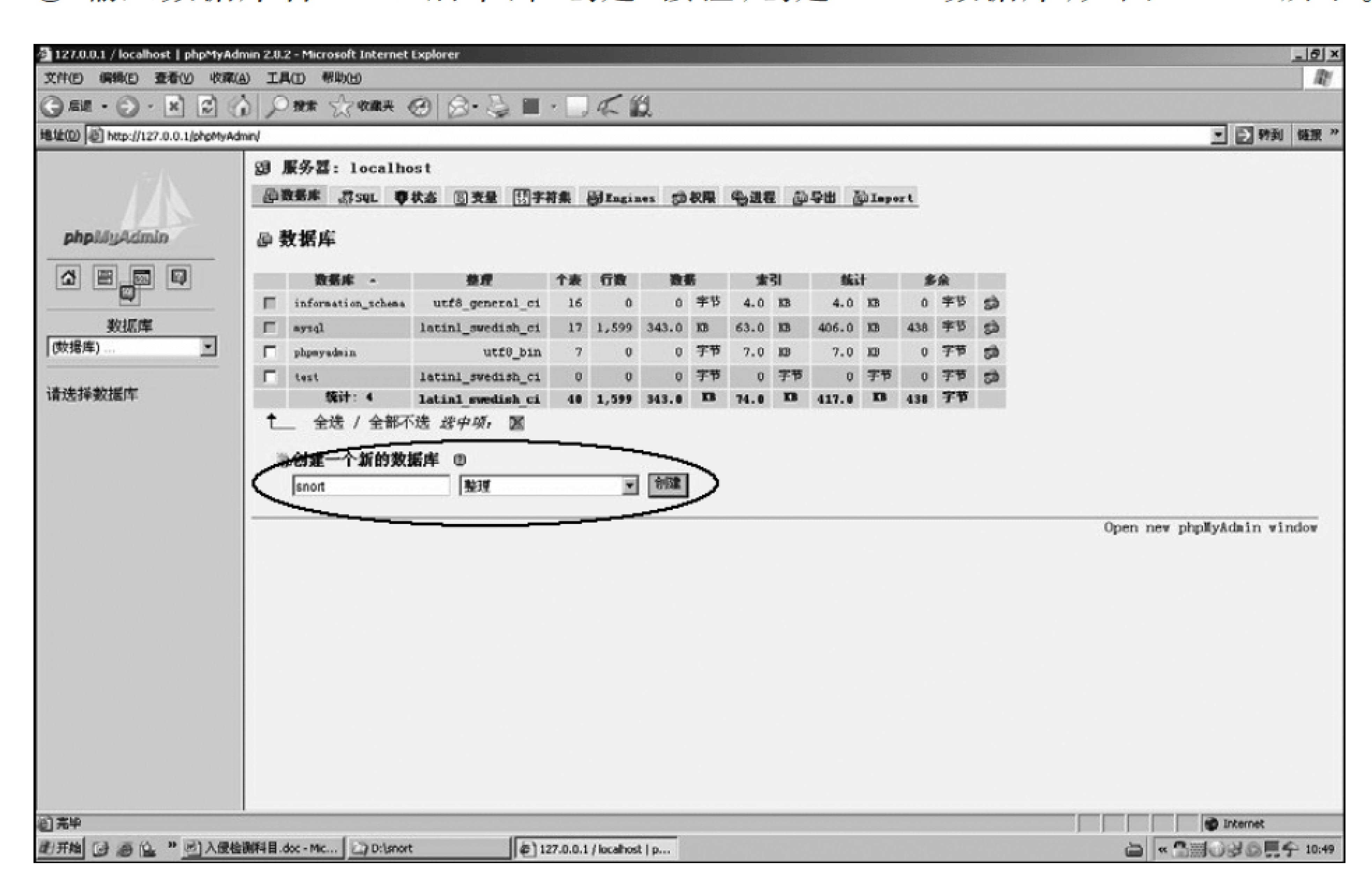


图 3-8-14 phpMyAdmin 创建数据库

③ 然后导入数据表脚本。单击 Import，如图 3-8-15 所示。

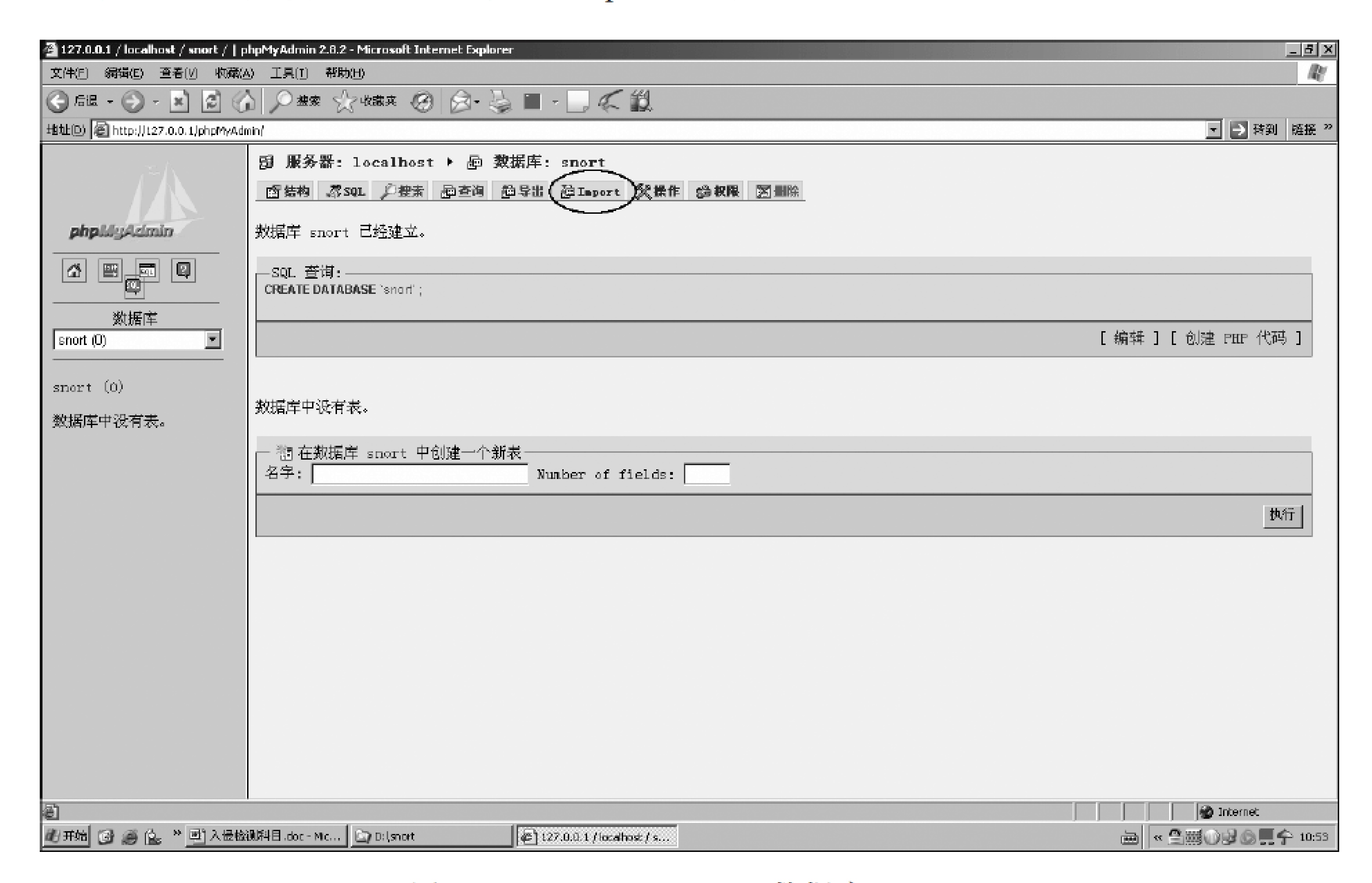


图 3-8-15 phpMyAdmin 数据库：Snort

④ 单击“浏览”按钮，找到 create_mysql（Snort 提供，光盘中自带）文件，单击“执行”按钮，为 Snort 数据库创建所有的数据表，如图 3-8-16 所示。

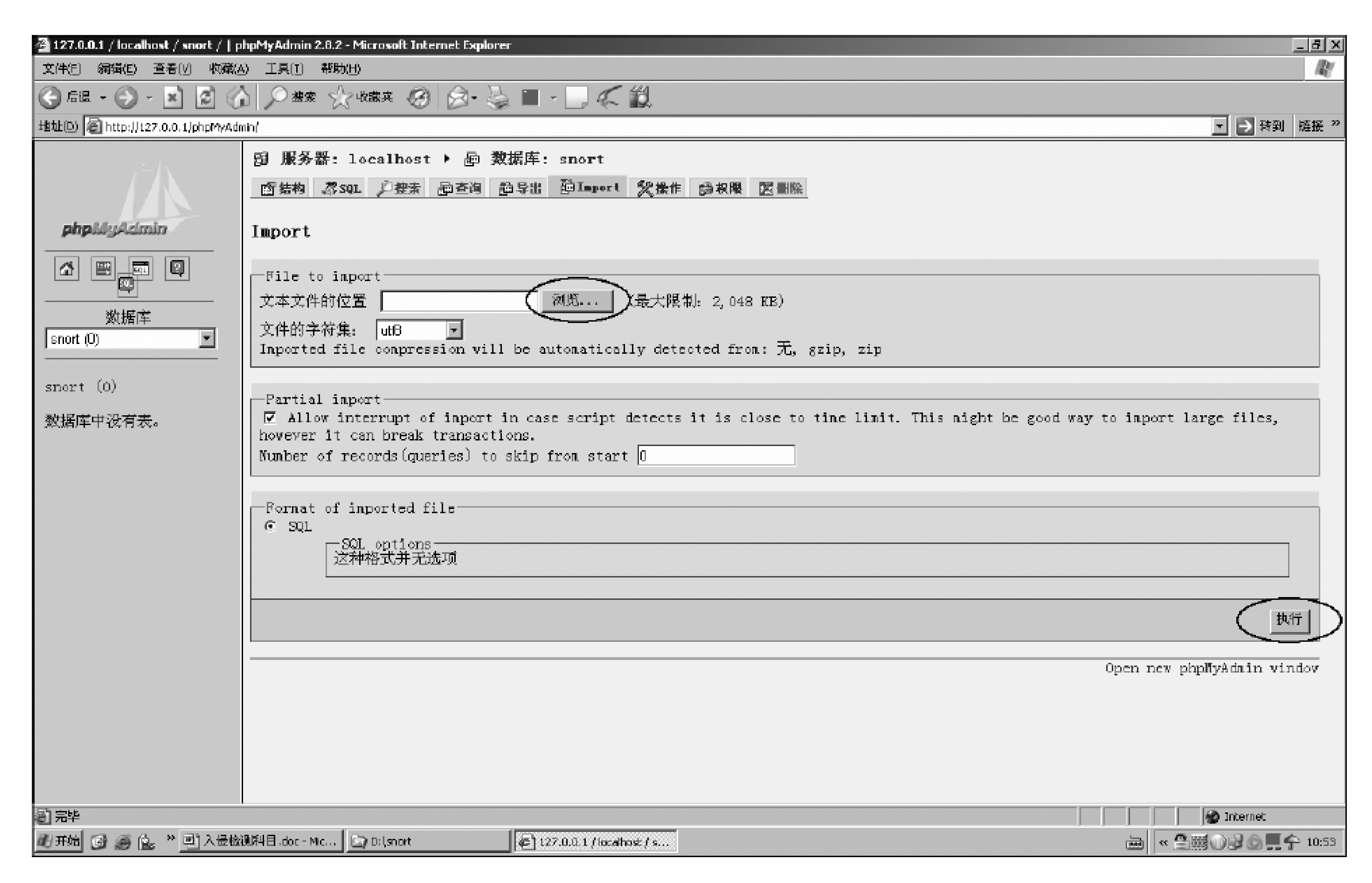


图 3-8-16 phpMyAdmin 数据库：snort-Import

⑤ 执行结果如图 3-8-17 所示。



图 3-8-17 phpMyAdmin 数据库：snort-Import 执行结果

(9) 设置 MySql 数据库用户。

① 单击“服务器：localhost”后单击“权限”按钮，如图 3-8-18 所示。

② 选择“添加新用户”为 Snort 入侵检测系统建立数据库用户，如图 3-8-19 所示。

③ 根据 Snort 入侵检测系统仅使用 Snort 数据库，所以设置 Snort 用户权限如下：

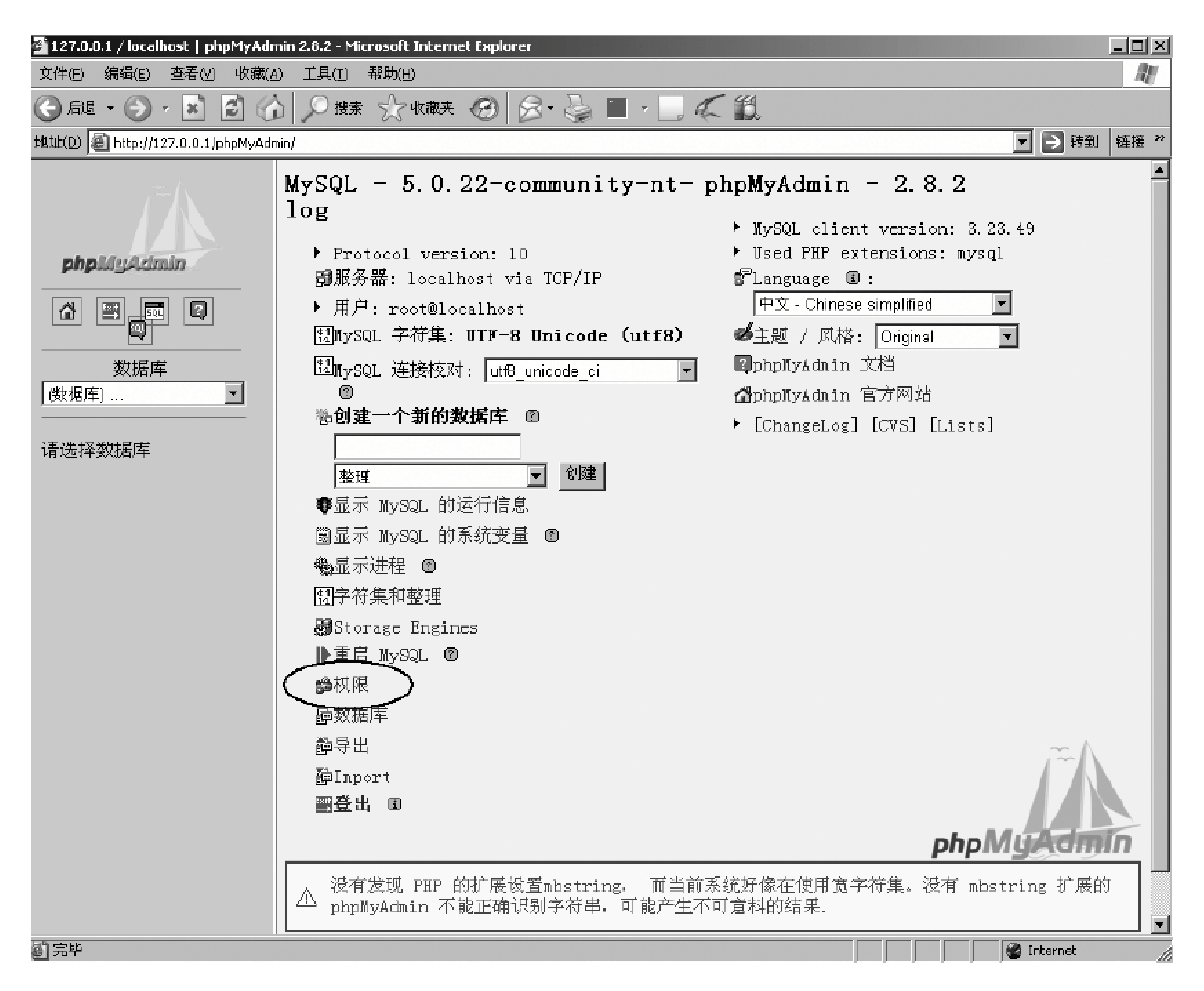


图 3-8-18　phpMyAdmin

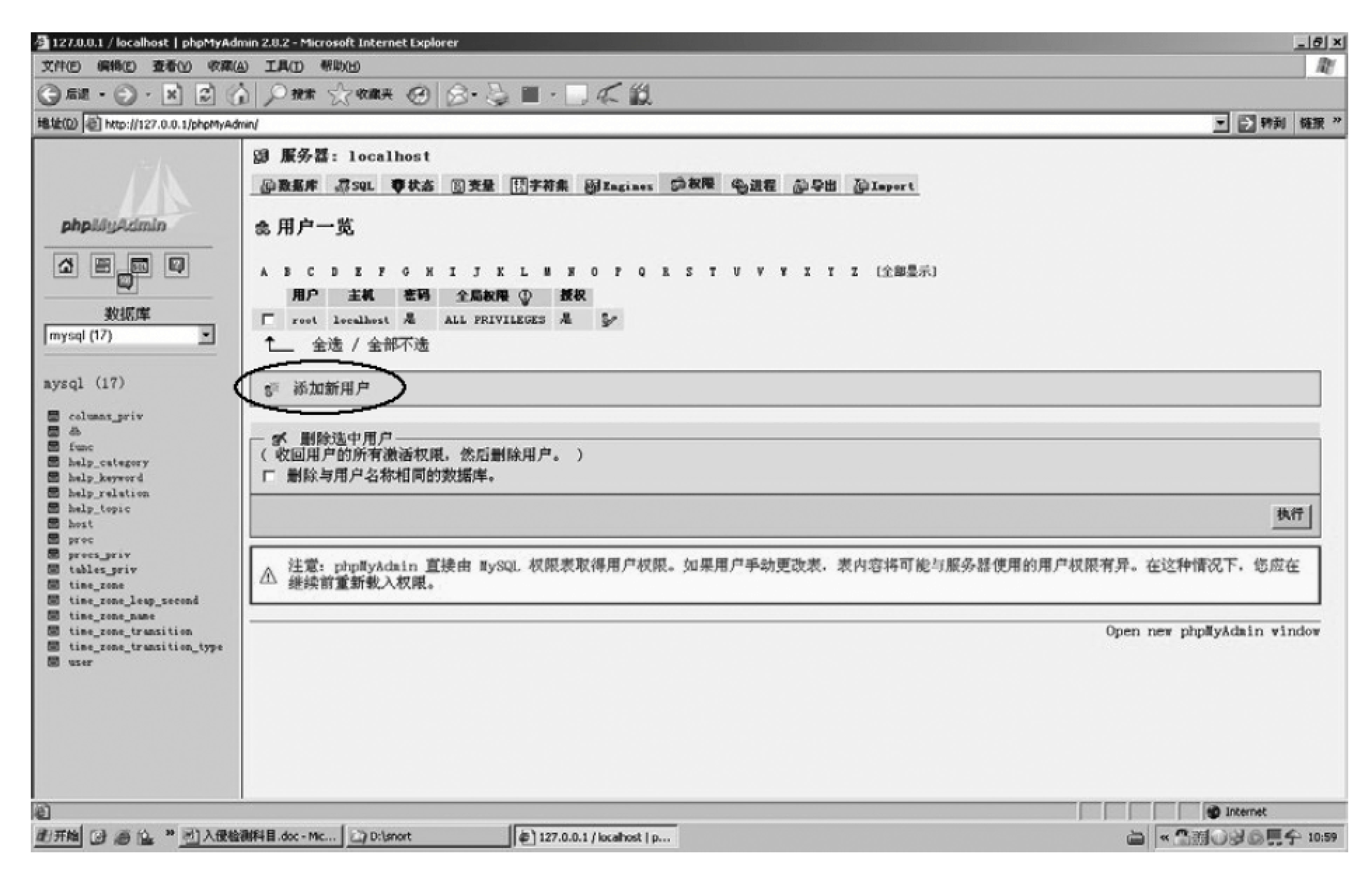


图 3-8-19　phpMyAdmin 权限

用户名：SnortUser。

密码：123456。

无须设置全局权限，单击“执行”按钮，如图 3-8-20 所示。



图 3-8-20　phpMyAdmin 权限添加新用户

④ 进入接下来的界面，在“按数据库指定权限组”选项框中选择 Snort 数据库，单击“执行”按钮，如图 3-8-21 所示。

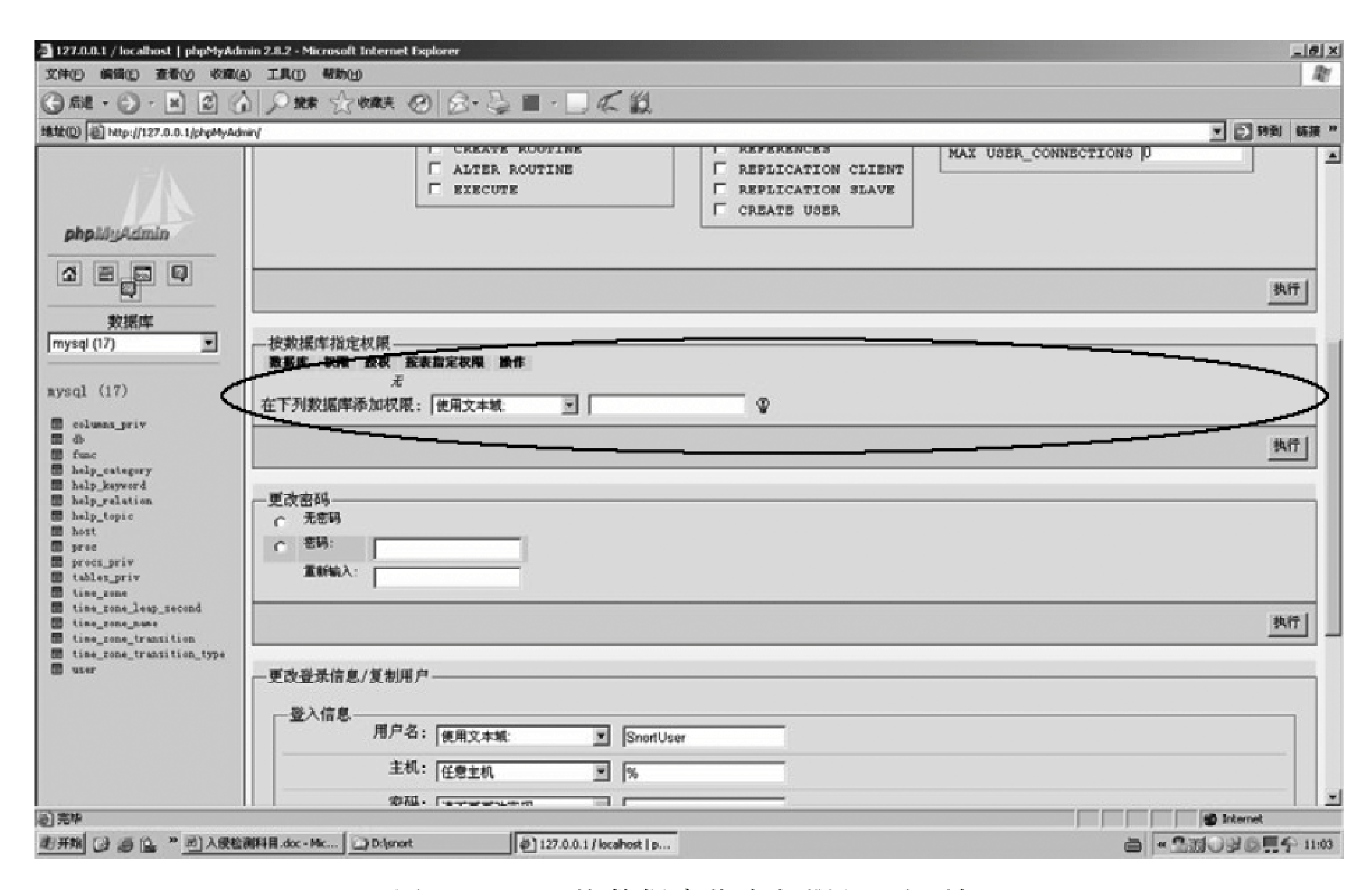


图 3-8-21　“按数据库指定权限组”选项框

⑤ 在“按数据库指定权限”选项框中选择所有的数据、结构和管理的所有权限，单击“执行”按钮，如图 3-8-22 所示。

⑥ 在单击权限时即可见具体的用户权限，如图 3-8-23 所示。

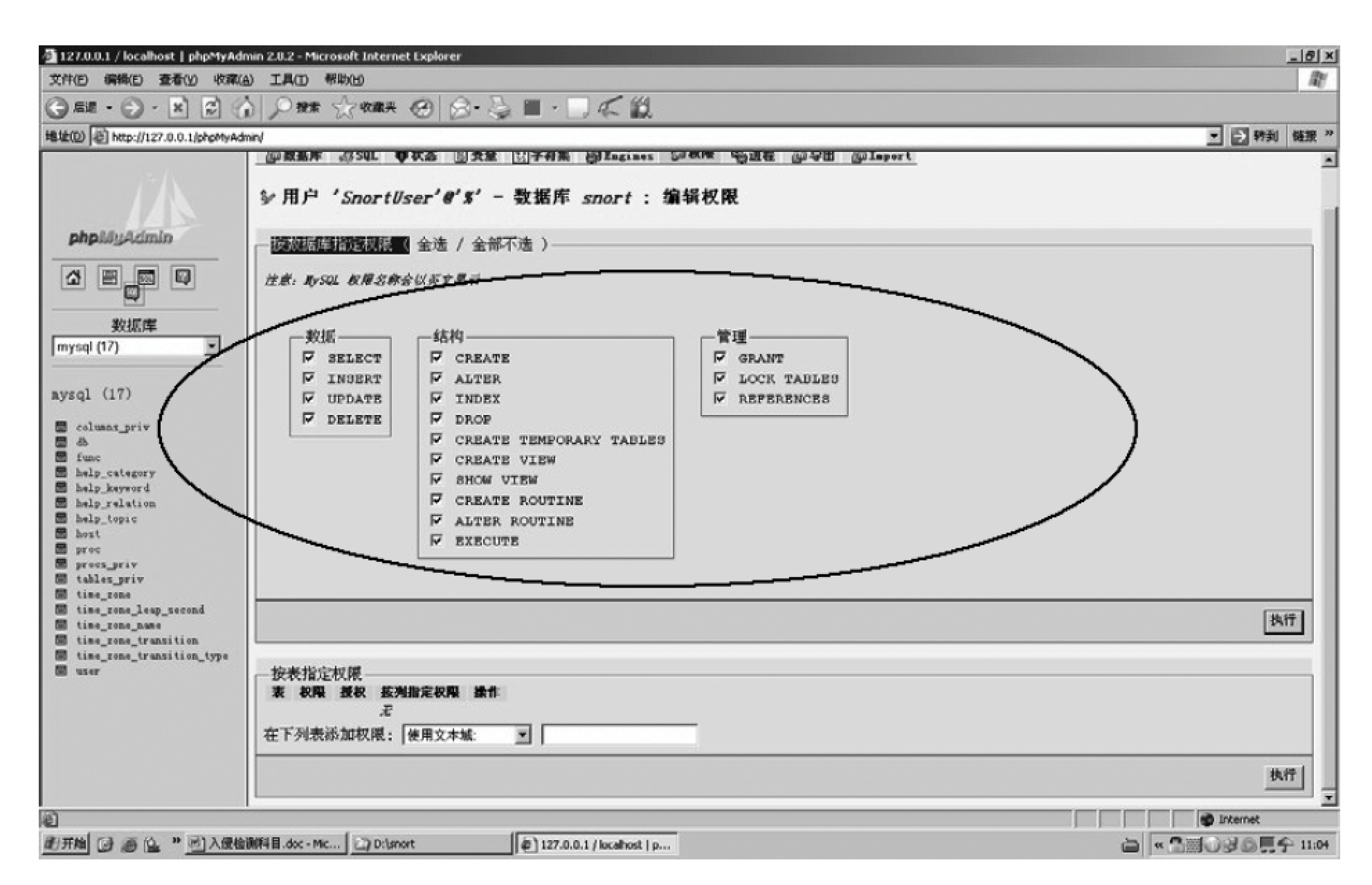


图 3-8-22　按数据库指定权限选项框

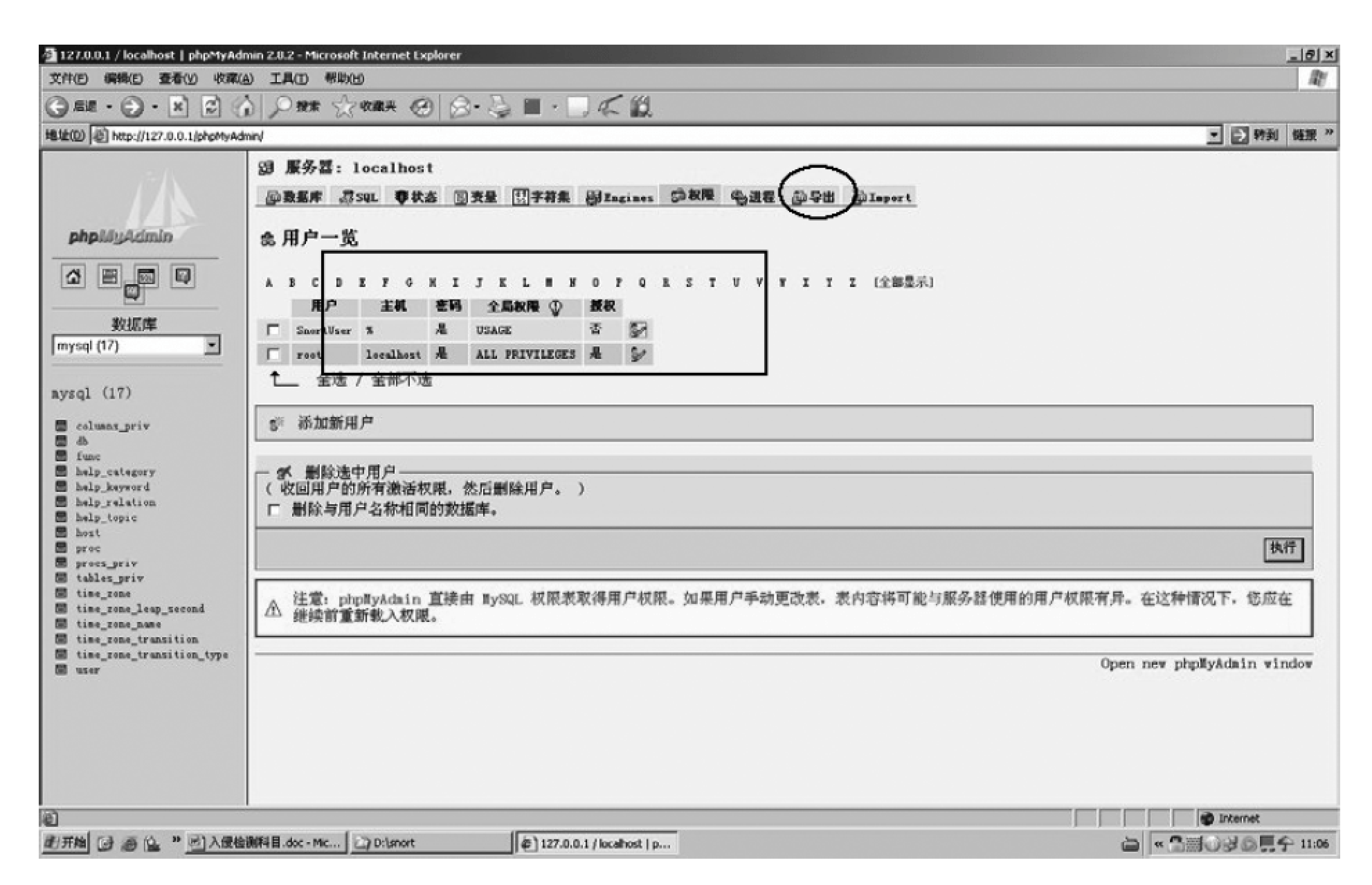


图 3-8-23　phpMyAdmin 服务器权限

⑦ 单击 SnortUser 后的“编辑”，可见 SnortUser 用户的权限，如图 3-8-24 所示。

(10) 安装 acid。

解压缩 acid-0.9.6b23.tar.gz 至 C:\Appserv\www\acid 目录中。

(11) 安装 jpgraph。

解压缩 jpgraph-1.20.5.tar.gz 至 C:\Appserv\php\jpgraph 目录中。

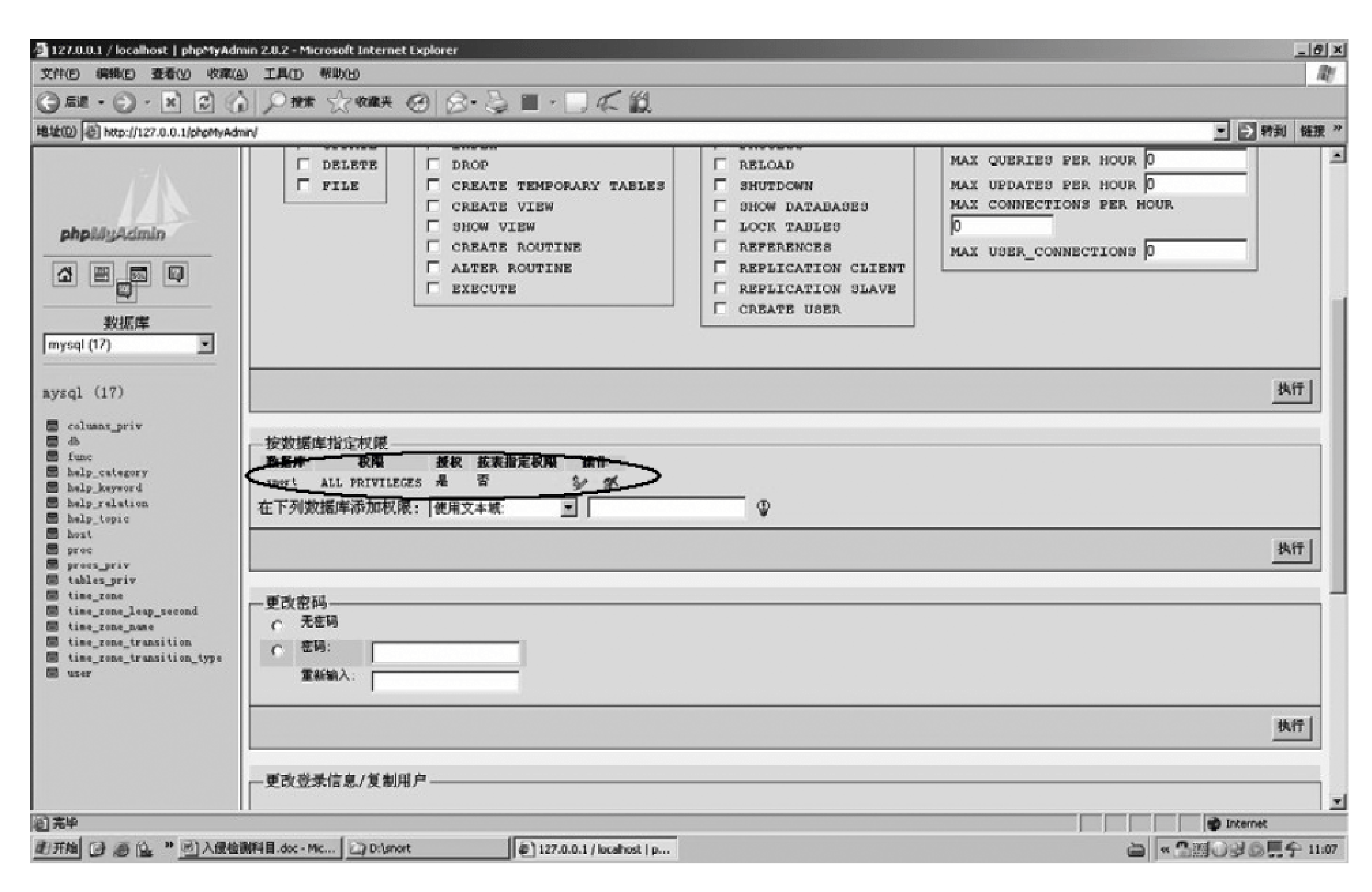


图 3-8-24　phpMyAdmin SnortUser 用户权限

（12）配置 acid。

编辑 C:\Appserv\www\acid\acid_conf. php 档案如下（利用寻找功能去修改字符串）。

```
$DBlib_path="c:\appserv\php\adodb"
$alert_dbname="snort";
$alert_host="localhost";
$alert_port="";
$alert_user="root";
$alert_password="123456";

$archive_dbname="snort";
$archive_host="localhost";
$archive_port="";
$archive_user="root";
$archive_password="123456";

$ChartLib_path="C:\AppServ\php\jpgraph\src";
```

（13）建立 acid 所需要的数据库。

使用 IE 进入 http://localhost/acid/acid_db_setup. php。依照页面提示单击 Create ACID AG 按钮建立即可，如图 3-8-25 所示。

（14）检测 acid 的安装情况。

打开 IE，访问 http://localhost/acid/，安装成功界面如图 3-8-26 所示。

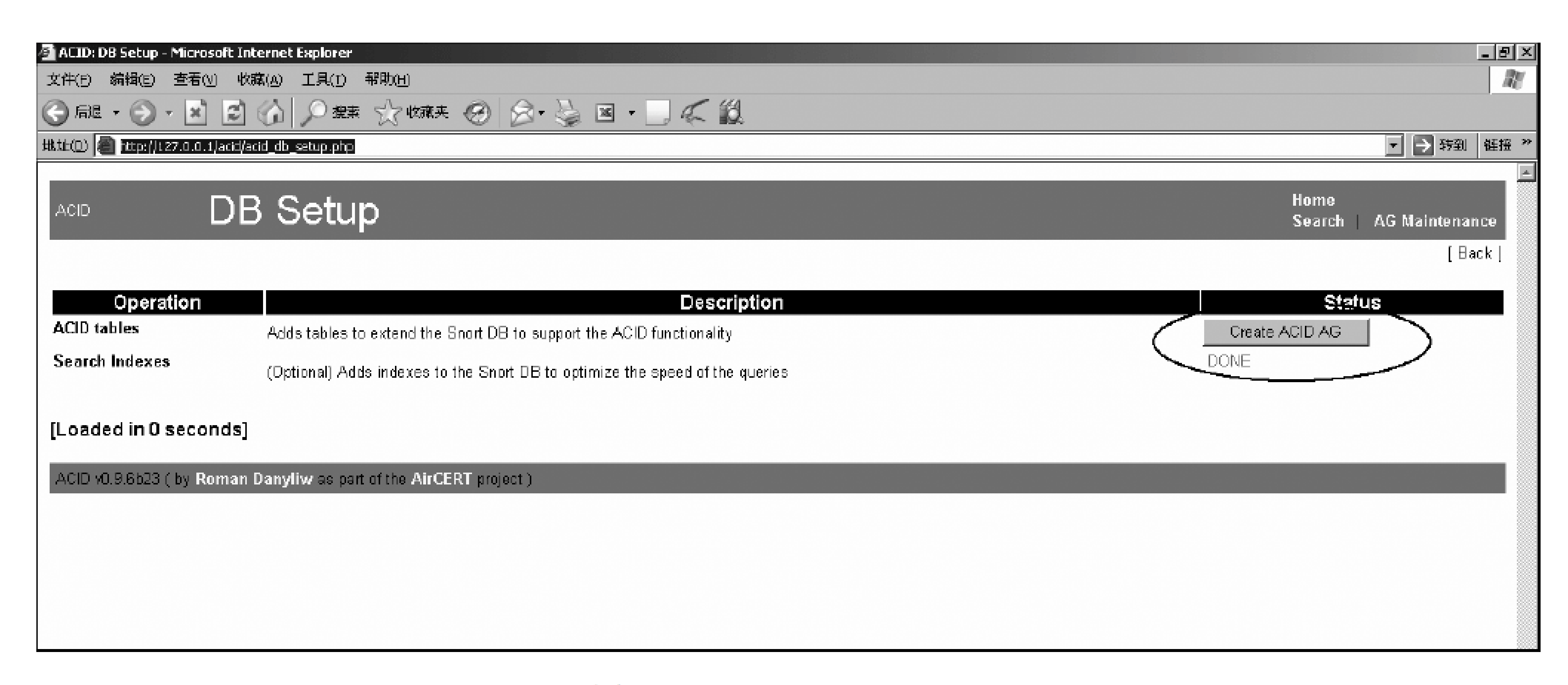


图 3-8-25　Acid DB Setup

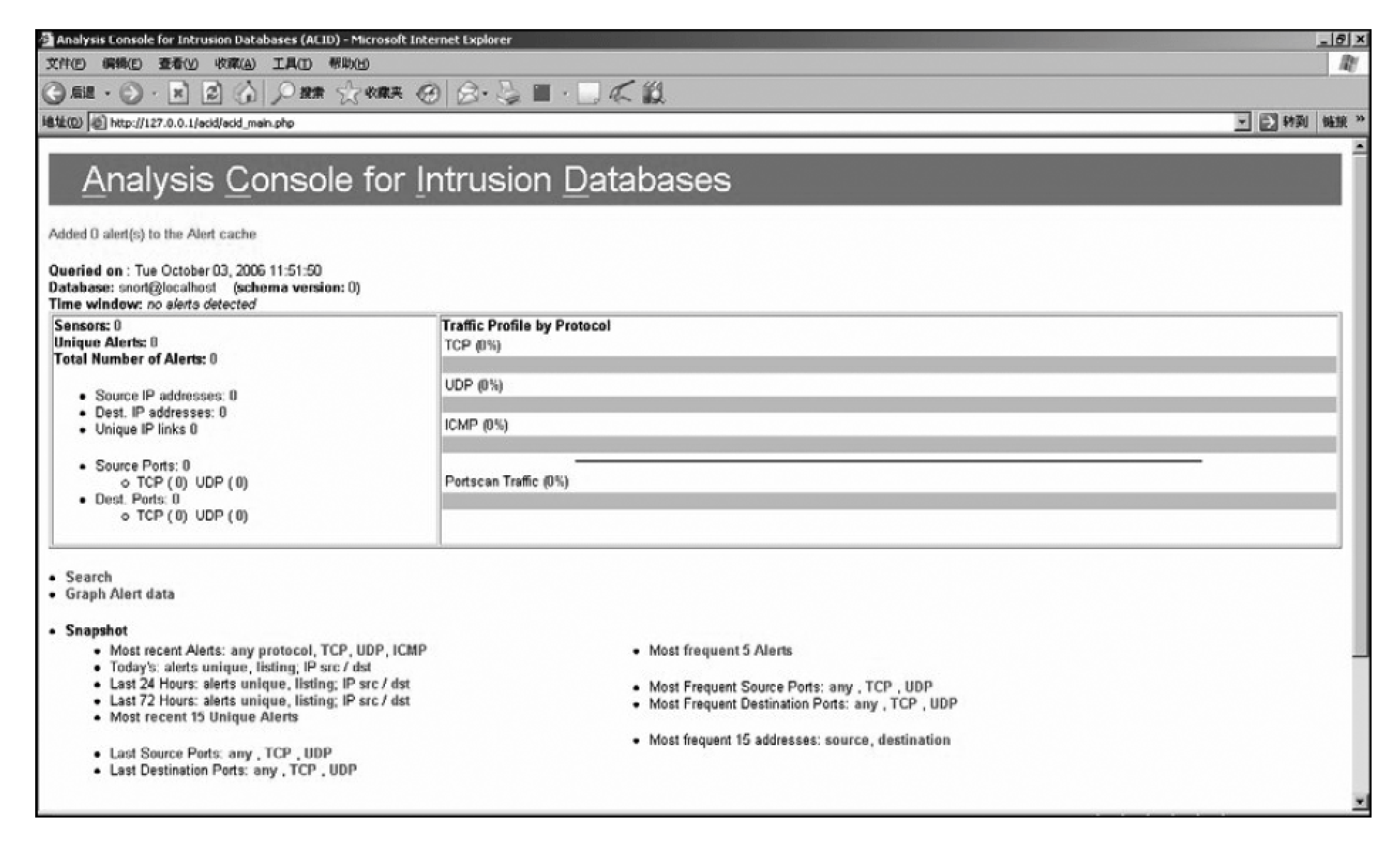


图 3-8-26　Acid Analysis Console for Intrusion Databases

(15) 安装 WinPcap。

打开 WinPcap_3_0. exe,根据向导安装即可。

(16) 安装 Snort。

打开 Snort_2_4_5_Installer. exe,根据向导安装,并采用默认目录安装 C:\Snort,如图 3-8-27 所示。

(17) 测试 Snort 的安装情况。

方法:打开 command 窗口,输入两条命令。

```
cd c:\snort\bin snort -v
```

将出现大量检测数据,如图 3-8-28 所示。

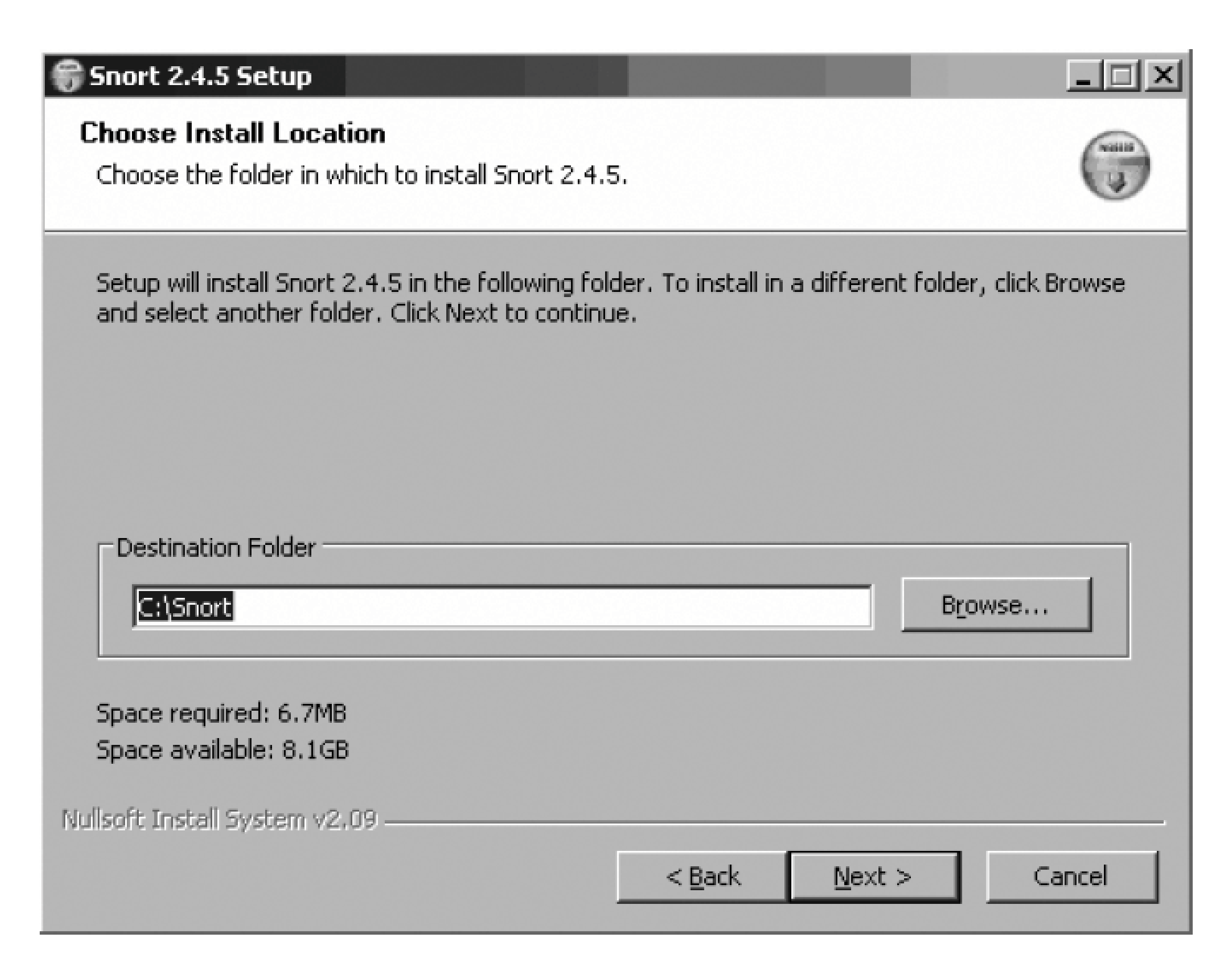


图 3-8-27　Snort 安装向导

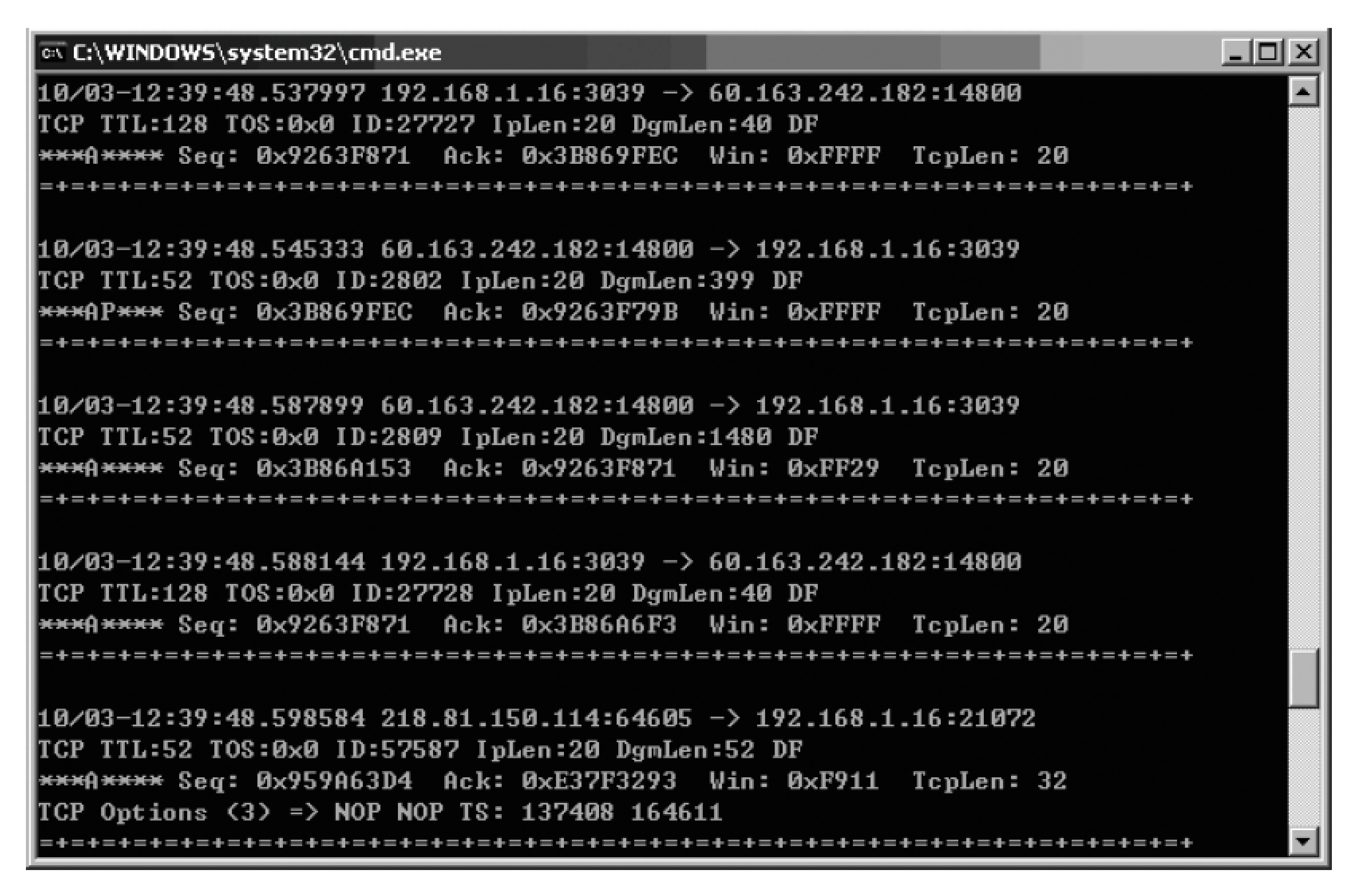


图 3-8-28　Snort-v 运行结果 1

按 Ctrl+C 组合键终止检测。可看到检测统计信息，如图 3-8-29 所示。

(18) 加载规则库。

解压 snortrules-pr-2.4.tar.gz，并复制 rules 目录到 C:/Snort/目录下覆盖原有的 rules。

(19) 配置 snort.conf 文件。

打开 C:\Snort\etc\snort.conf 文件，编辑如下：

```
var RULE_PATH c:\snort\rules        //给出 rules 的位置
var HOME_NET any                    //any 改成本机器 IP: 192.168.1.16/24
```

```
var HTTP_PORTS 80                //根据自身设置修改

#output database: log,mysql,user= root password= test dbname= db host= localhost
#output database: alert,postgresql,user= snort dbname= snort
//去掉#,根据自身设置修改
//本例为
output database: log,mysql,user= SnortUser password= 123456 dbname= snort host= 192.168.1.16(MySQL数据库安装的机器 IP)
output database: alert, mysql,user= SnortUser password= 123456 dbname= snort host= 192.168.1.16(MySQL数据库安装的机器 IP)
```

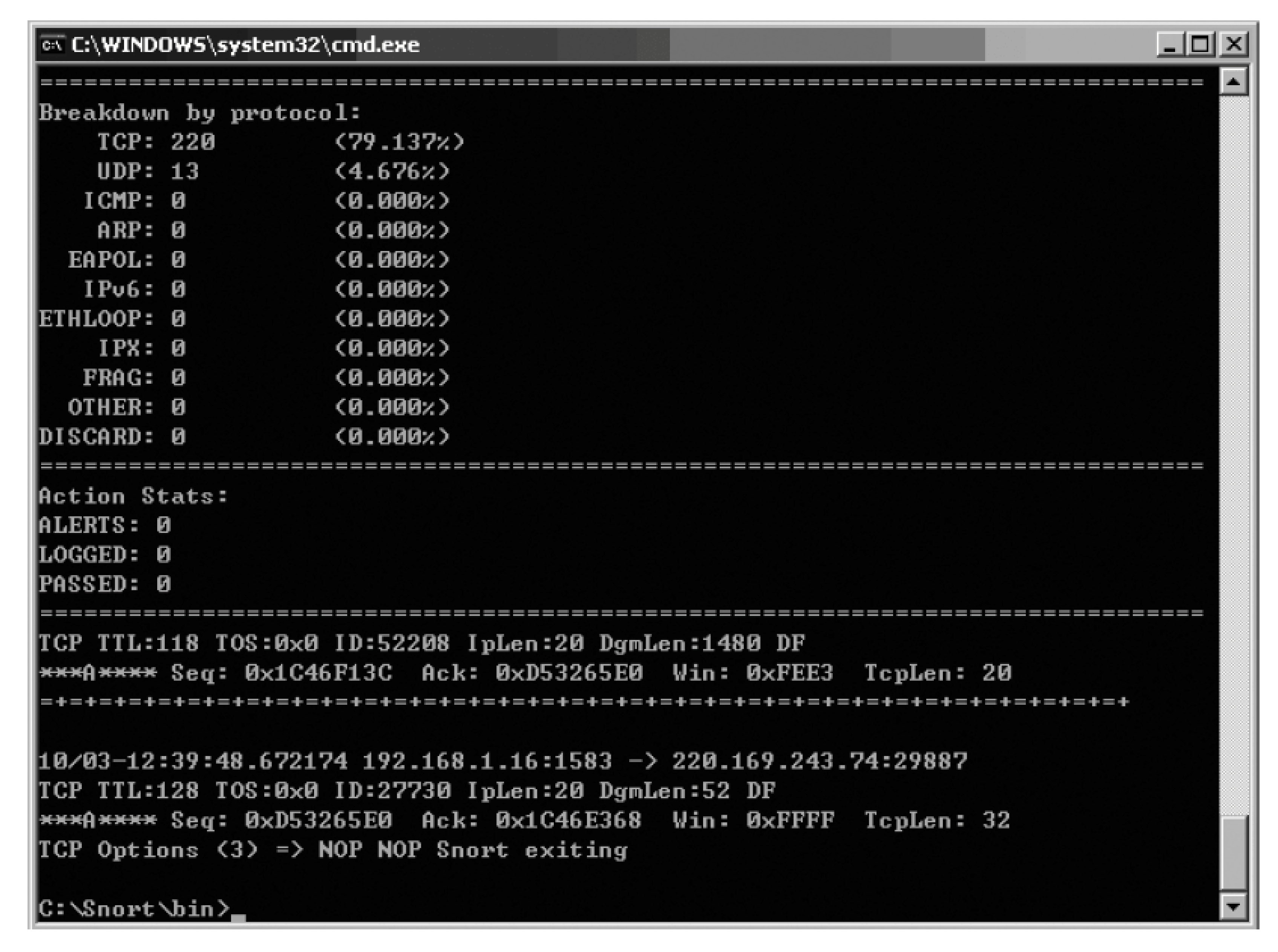


图 3-8-29 Snort-v 运行结果 2

(20) 建立运行 Snort 批处理文件。

在 C:/Snort/bin 目录下建立 runsnort. bat,在文件中输入“Snort -c"c:\snort\etc\snort. conf" -l"c:\snort\log" -d -e -X”(注：若数据库存储有误,可增加参数-U,该问题由 snort 版本不同引起)。

然后在 C:/Snort/bin 目录下运行 runsnort,即可根据配置运行 Snort 入侵检测系统。

测试效果：可以通过 IE 输入 http://192. 168. 1. 16/acid 观察检测结果,如图 3-8-30 所示。

3.8.8 实验思考

入侵检查系统的误报和漏报是怎样产生的？误报率和漏报率二者之间的关系怎样？

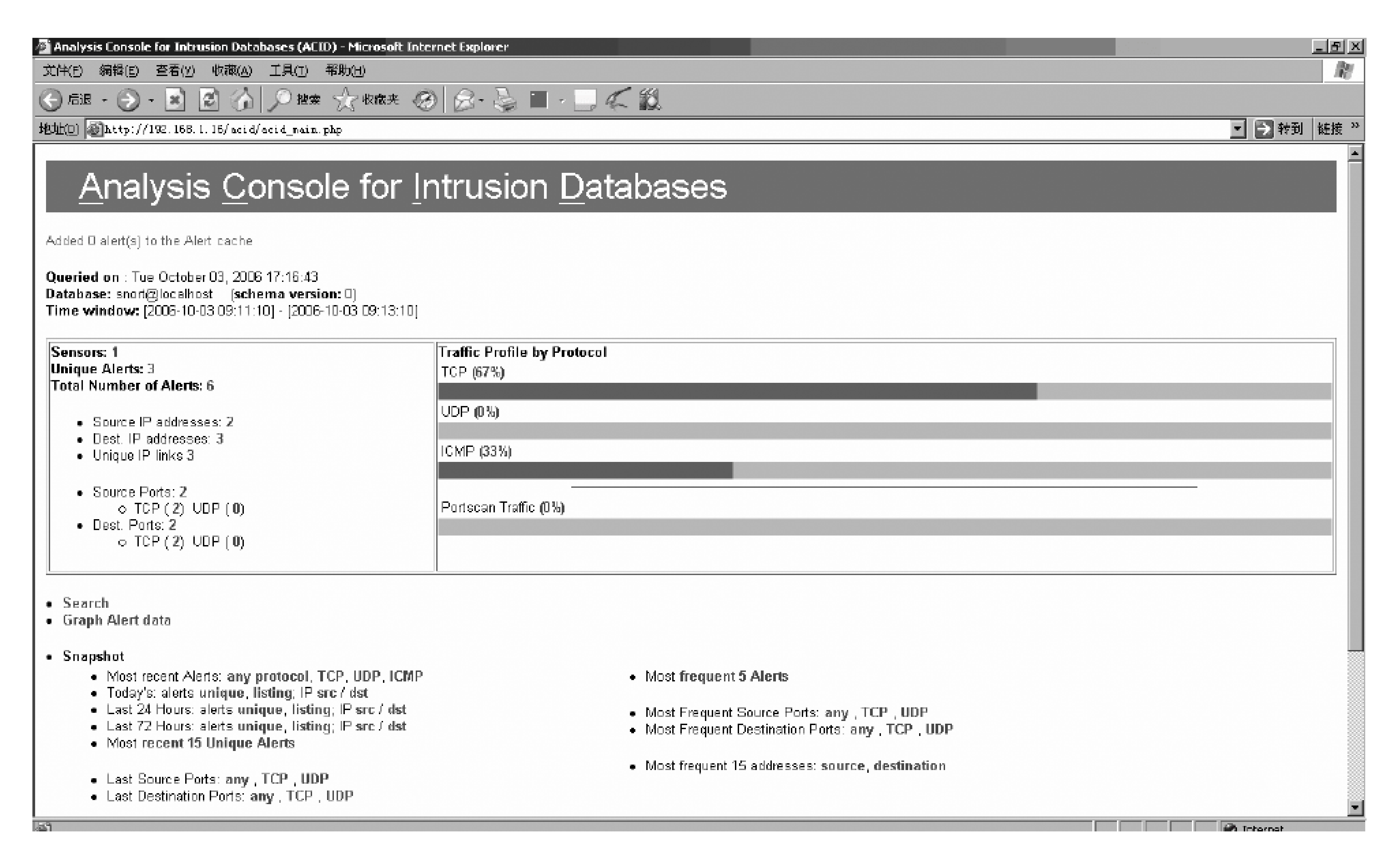


图 3-8-30 http://192.168.1.16/acid 运行结果

3.9 Internet 服务器安全

3.9.1 实验类型

综合型,4 学时,必选实验。

3.9.2 实验目的

通过实验,使学生能够对 Internet 服务器进行安全的配置与管理。

3.9.3 题目描述

对 Windows Server 2003 Web 服务器进行安全加固。

3.9.4 实验要求

能够配置比较安全的 Web 服务器。

3.9.5 相关知识

所谓“兵马未发,粮草先行”,在安装和配置一个 Internet 服务器之前,首先要从思想

上对安全工作有个全局认识，至少应该考虑好以下几个方面的内容。

1）编制计划

编制安装计划的过程本身就可以作为一篇论文深加论述，这里只做概要介绍。保护Internet服务器安全需要详尽的计划，这不是指在安装过程中弹出菜单时确定选择哪一个项目，而是要仔细确定系统的功能和目标，最终成为安装的路标、排除故障的向导、服务器安装及网络边界情况的基础文档。如果需要安装计划编制方面的基础性方针资料，可以参考RFC手册之2196项“站点安全手册”，地址是http://www.faqs.org/rfcs/rfc2196.html。

2）设计策略

除了确定服务器将执行哪些功能，还需要确定谁能访问服务器、在服务器上存储什么数据以及在出现各种情况时应该采取哪些措施。这就是策略的制订。实际上，策略定义了一个组织的服务器与接受它的服务和数据的Internet公众之间的交互作用细节。真正安全的站点必须具有适当的策略。关于策略的设计，同样请参考RFC手册之2196项“站点安全手册”。

3）访问控制

这方面是指对服务器的访问权，主要包括三类。

（1）物理访问控制：指实际接触和操作服务器控制台的能力。如果攻击者取得了物理访问权，就可以绕过许多安全措施，整个安全计划将出现一个大大的漏洞。

（2）系统访问控制：确定哪些组或个人账号对系统拥有何种权限，例如备份和恢复数据、向Web服务器发布文档、管理账户或组。

（3）网络访问控制：网络访问控制规定了内部网与Internet相互作用的权限，例如端口访问、数据读取、服务使用等。不仅要考虑到外部的入侵行为，还要设想到内部的敌人攻击。为此，一般将服务器放在DMZ区域内。一个DMZ（Demilitarized Zone）就是一个孤立的网络，可以把不信任的系统放在那里。例如，希望任何人都能访问Web和E-mail服务器，所以它们就是不能信任的；将它们放在DMZ中特别关照，就可对来自内部和外部的访问都进行限制。

3.9.6 实验设备

主流配置PC一台，Windows 2003 Server操作系统，网络环境。

3.9.7 实验步骤

（1）安装和配置Windows Server 2003。

① 将<systemroot>\System32\cmd.exe转移到其他目录或更名。

② 系统账号尽量少，更改默认账户名（如Administrator）和描述，密码尽量复杂。

③ 拒绝通过网络访问该计算机（匿名登录；内置管理员账户；Support_388945a0；Guest；所有非操作系统服务账户）。

④ 建议对一般用户只给予读取权限，而只给管理员和System以完全控制权限，但这

样做有可能使某些正常的脚本程序不能执行，或者某些需要写的操作不能完成，这时需要对这些文件所在的文件夹权限进行更改，建议在做更改前先在测试机器上作测试，然后慎重更改。

⑤ NTFS 文件权限设定(注意文件的权限优先级别比文件夹的权限高)，如表 3-9-1 所示。

表 3-9-1 NTFS 文件权限设定

文件类型	建议的 NTFS 权限
CGI 文件(.exe、.dll、.cmd、.pl)脚本文件(.asp)包含文件(.inc、.shtm、.shtml)静态内容(.txt、.gif、.jpg、.htm、.html)	Everyone(执行) Administrators(完全控制) System(完全控制)

• 操作提示：右击需要设定访问权限的文件夹，选择"共享和安全"，如图 3-9-1 所示。



图 3-9-1 设置用户的访问权限

⑥ 禁止 C$、D$一类的默认共享。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameter s AutoShareServer、REG_DWORD、0x0

• 操作提示：单击"开始"菜单，选择"运行"，在输入框中输入"regedit"后按 Enter 键，打开"注册表编辑器"，如图 3-9-2 所示。

步骤⑥～⑧、⑭～㉒按此操作方式进行设置。

⑦ 禁止 ADMIN$默认共享。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameter s AutoShareWks、REG_DWORD、0x0

⑧ 限制 IPC$默认共享。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa restrictanonymous REG_DWORD 0x0 默认



图 3-9-2　注册表编辑器

0x1 匿名用户无法列举本机用户列表

0x2 匿名用户无法连接本机 IPC＄共享

说明：不建议使用 0x2，否则可能会造成一些服务无法启动，如 SQL Server。

⑨ 仅给用户真正需要的权限，权限的最小化原则是安全的重要保障。

⑩ 在“本地安全策略”→“审核策略”中打开相应的审核，推荐的审核是：

账户管理 成功 失败

登录事件 成功 失败

对象访问 失败

策略更改 成功 失败

特权使用 失败

系统事件 成功 失败

目录服务访问 失败

账户登录事件 成功 失败

审核项目少的缺点是当你想看发现没有记录；审核项目太多不仅会占用系统资源，而且会导致你根本没空去看，这样就失去了审核的意义了。

与之相关的是：在“账户策略”→“密码策略”中设定如下：

密码复杂性要求启用。

密码长度最小值 6 位。

强制密码历史 5 次。

最长存留期 30 天。

在“账户策略”→“账户锁定策略”中设定如下：

账户锁定 3 次错误登录。

锁定时间 20 分钟。

复位锁定计数 20 分钟。

- 操作提示：单击“开始”菜单，选择“运行”，在输入框中输入“regedit”后按 Enter 键，打开“注册表编辑器”，如图 3-9-3 所示。

⑪ 在 Terminal Service Configuration(远程服务配置)→权限→高级中配置“安全审核”，一般来说只要记录登录、注销事件就可以了。



图 3-9-3 本地安全策略设置

⑫ 解除 NetBios 与 TCP/IP 协议的绑定。控制面板→网络→绑定→NetBios 接口→禁用 2000：控制面板→网络和拨号 连接→本地网络→属性→TCP/IP→属性→高级→WINS→禁用 TCP/IP 上的 NETBIOS。

⑬ 在网络连接的协议里启用 TCP/IP 筛选，仅开放必要的端口(如 80)。

⑭ 通过更改注册表来禁止 139 空连接。

Local_Machine\System\CurrentControlSet\Control\LSA-RestrictAnonymous=1

⑮ 修改数据包的生存时间(TTL)值。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters DefaultTTL REG_DWORD 0-0xff (0-255 十进制，默认值 128)

⑯ 防止 SYN 洪水攻击。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters SynAttackProtect REG_DWORD 0x2(默认值为 0x0)

⑰ 禁止响应 ICMP 路由通告报文。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfa ces\interface PerformRouterDiscovery REG_DWORD 0x0(默认值为 0x2)

⑱ 防止 ICMP 重定向报文的攻击。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters EnableICMPRedirects REG_DWORD 0x0(默认值为 0x1)

⑲ 不支持 IGMP 协议。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters IGMPLevel REG_DWORD 0x0(默认值为 0x2)

⑳ 设置 arp 缓存老化时间设置。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters ArpCacheLife REG_DWORD 0-0xFFFFFFFF(秒数,默认值为 120 秒)

ArpCacheMinReferencedLife REG_DWORD 0- 0xFFFFFFFF(秒数,默认值为 600)

㉑ 禁止死网关监测技术。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters EnableDeadGWDetect REG_DWORD 0x0(默认值为 0x1)

㉒ 不支持路由功能。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters IPEnableRouter REG_DWORD 0x0(默认值为 0x0)

(2) 安装和配置 IIS 服务。

① 仅安装必要的 IIS 组件(禁用不需要的如 FTP 和 SMTP 服务)。

• 操作提示:有两种方法如下。

■方法一:单击“开始”菜单,选择“设置”→“控制面板”→“添加或删除程序”→“添加/删除 Windows 组件”→“应用程序服务器”,按提示进行安装,如图 3-9-4 所示。

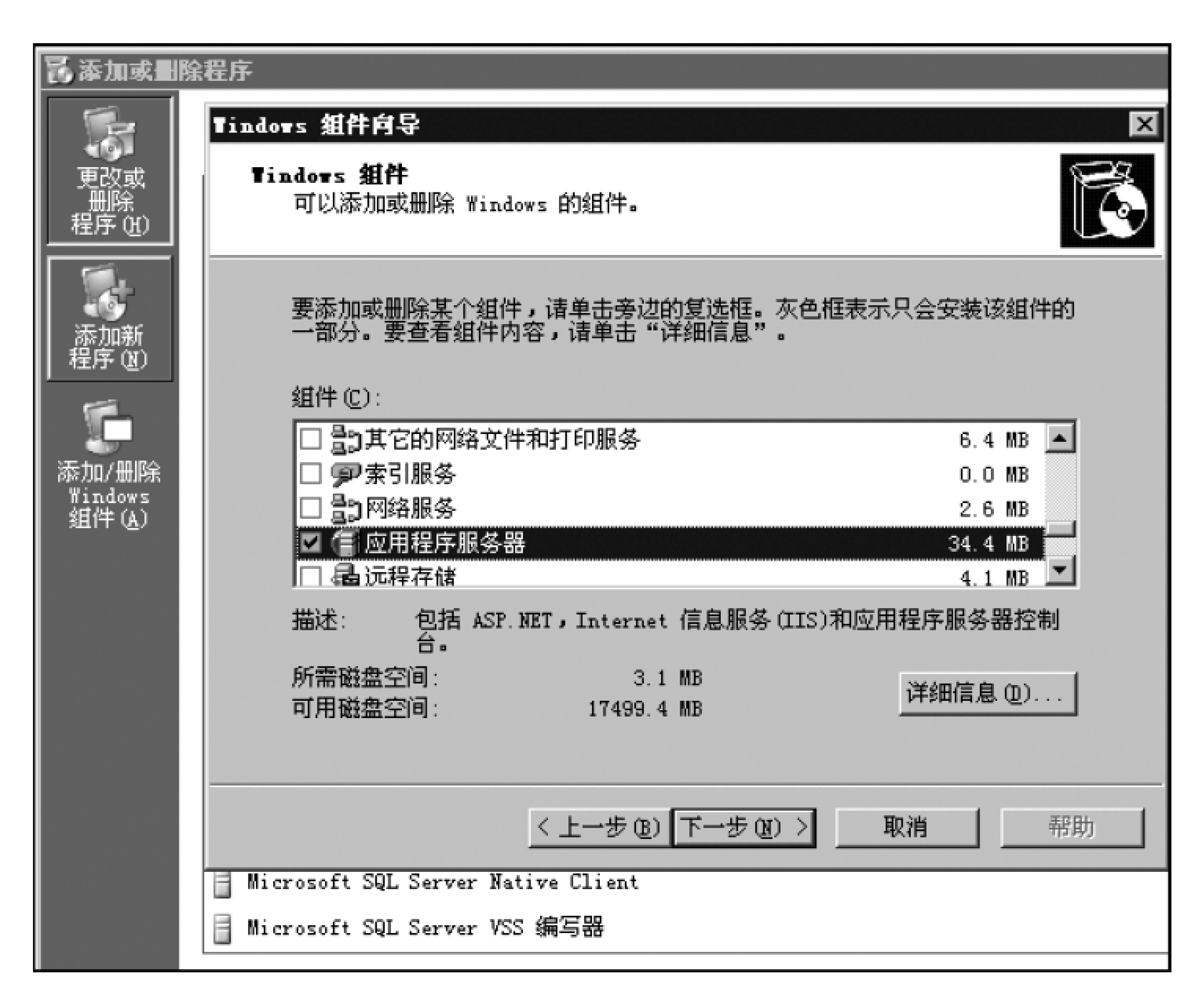


图 3-9-4 通过添加或删除程序安装 IIS

■方法二:双击桌面“管理您的服务器”快捷方式,选择“添加或删除角色”,如图 3-9-5所示。

出现“配置您的服务器向导”对话框,如图 3-9-6 所示。

单击“下一步”按钮,在“配置您的服务器向导”中选择“应用程序服务器(IIS,ASP.NET)”,单击“下一步”按钮,按提示进行安装,如图 3-9-7 所示。

② 仅启用必要的服务和 Web Service 扩展,推荐配置,如表 3-9-2 所示。

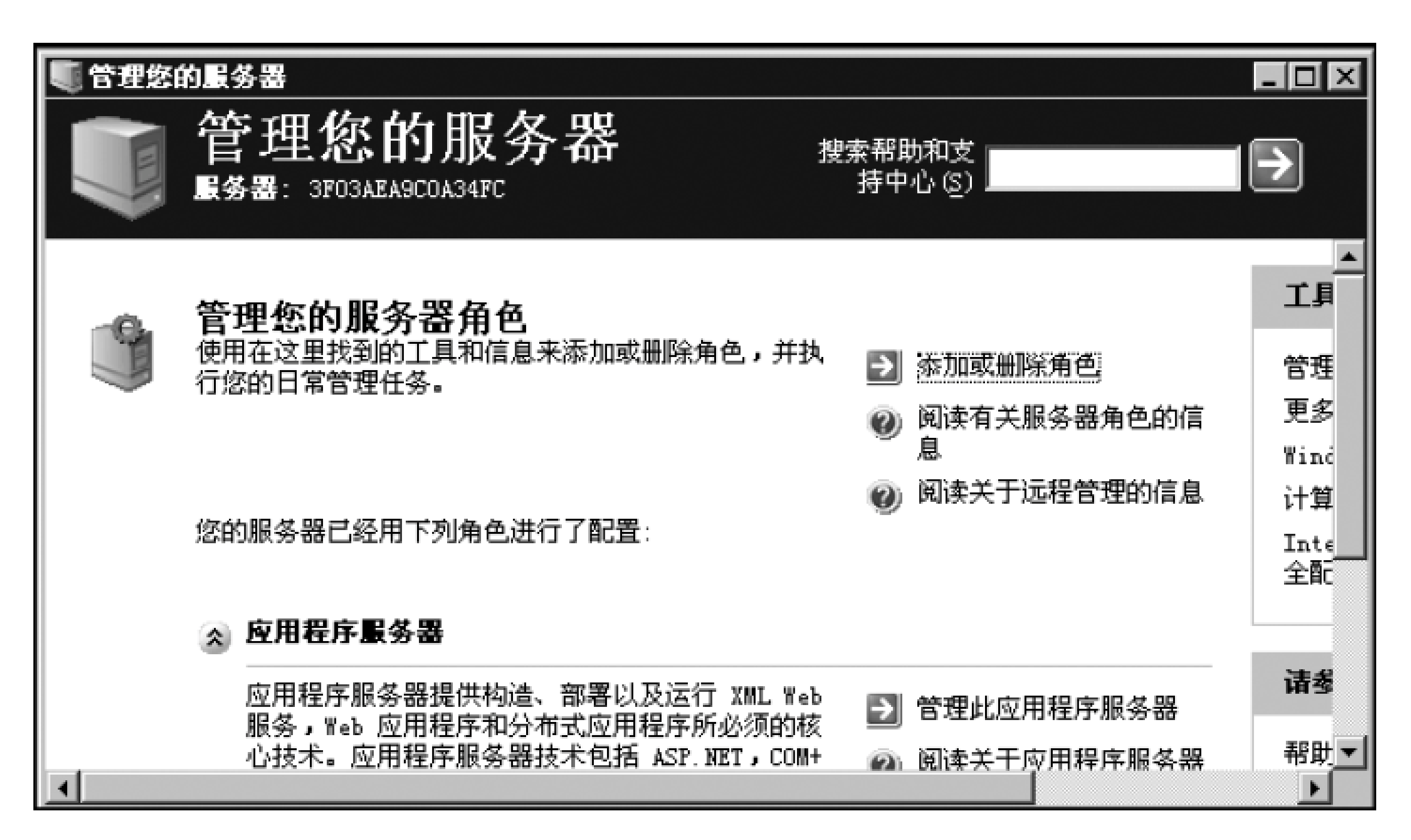


图 3-9-5　管理服务器方式安装 IIS

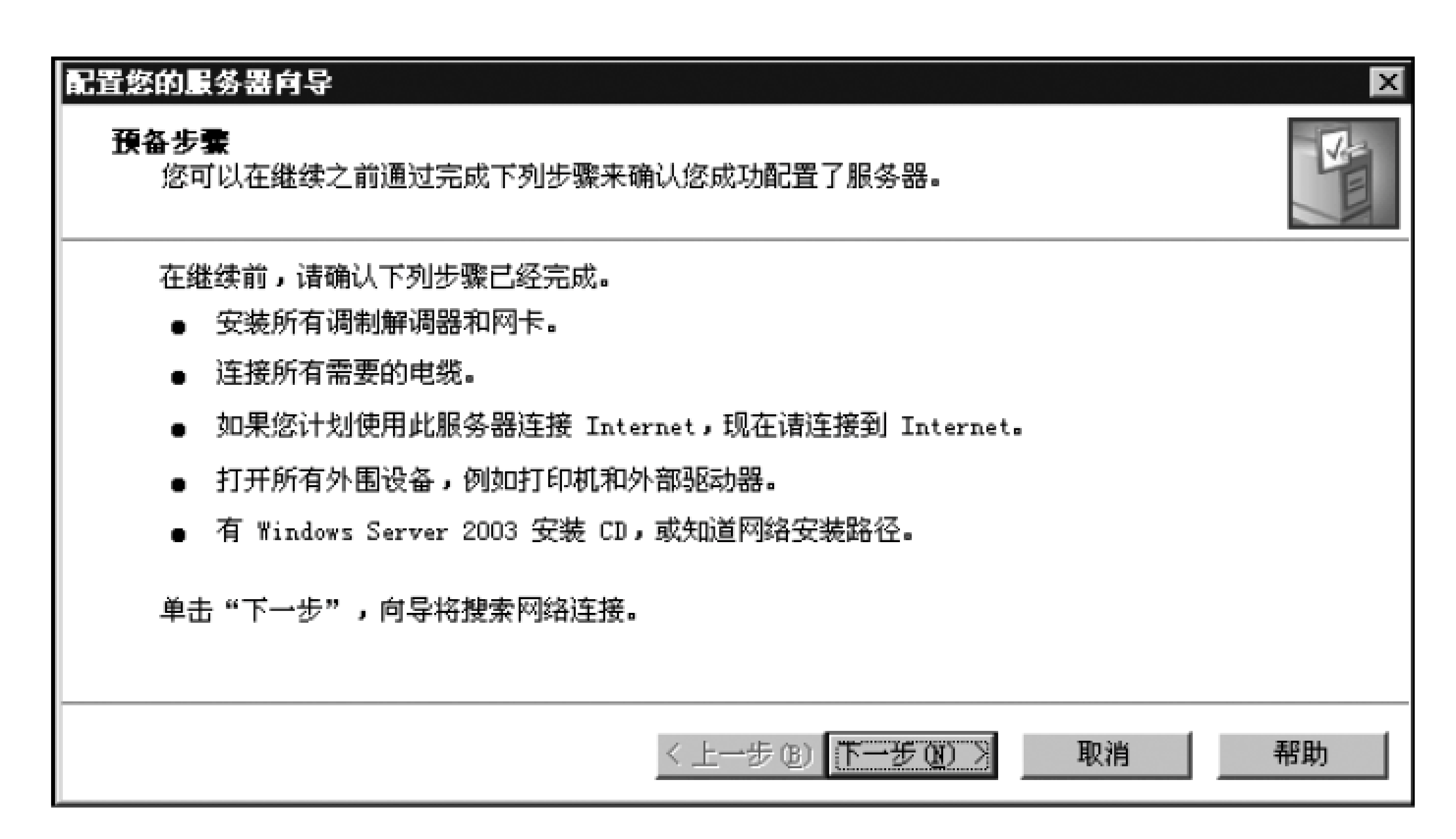


图 3-9-6　配置服务器向导

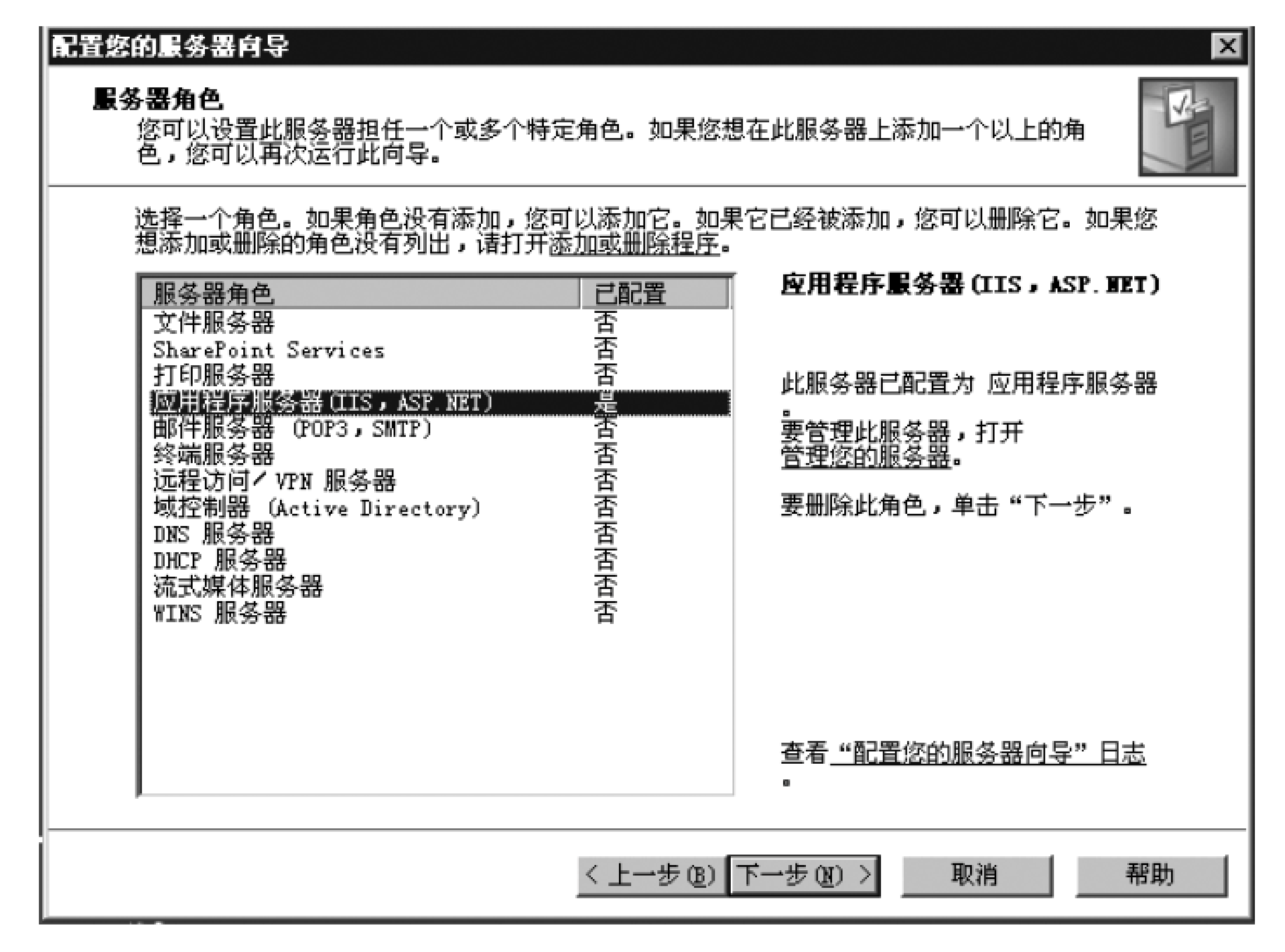


图 3-9-7　选择“应用程序服务器”

表 3-9-2　IIS 组件配置

UI 中的组件名称	设置	设置逻辑
后台智能传输服务(BITS)服务器扩展	启用	BITS 是 Windows Updates 和“自动更新”所使用的后台文件传输机制。如果使用 Windows Updates 或“自动更新”在 IIS 服务器中自动应用 Service Pack 和热修补程序，则必须有该组件
公用文件	启用	IIS 需要这些文件，一定要在 IIS 服务器中启用它们
文件传输协议(FTP)服务	禁用	允许 IIS 服务器提供 FTP 服务。专用 IIS 服务器不需要该服务
FrontPage 2002 Server Extensions	禁用	为管理和发布 Web 站点提供 FrontPage 支持。如果没有使用 FrontPage 扩展的 Web 站点，请在专用 IIS 服务器中禁用该组件
Internet 信息服务管理器	启用	IIS 的管理界面
Internet 打印	禁用	提供基于 Web 的打印机管理，允许通过 HTTP 共享打印机。专用 IIS 服务器不需要该组件
NNTP 服务	禁用	在 Internet 中分发、查询、检索和投递 Usenet 新闻文章。专用 IIS 服务器不需要该组件
SMTP 服务	禁用	支持传输电子邮件。专用 IIS 服务器不需要该组件
万维网服务	启用	为客户端提供 Web 服务、静态和动态内容。专用 IIS 服务器需要该组件

③ 万维网服务子组件如表 3-9-3 所示。

表 3-9-3　万维网服务子组件配置

UI 中的组件名称	安装选项	设置逻辑
Active Server Page	启用	提供 ASP 支持。如果 IIS 服务器中的 Web 站点和应用程序都不使用 ASP，请禁用该组件；或使用 Web 服务扩展禁用它
Internet 数据连接器	禁用	通过扩展名为.idc 的文件提供动态内容支持。如果 IIS 服务器中的 Web 站点和应用程序都不包括.idc 扩展文件，请禁用该组件；或使用 Web 服务扩展禁用它
远程管理(HTML)	禁用	提供管理 IIS 的 HTML 界面。改用 IIS 管理器可使管理更容易，并减少了 IIS 服务器的攻击面。专用 IIS 服务器不需要该功能
远程桌面 Web 连接	禁用	包括了管理终端服务客户端连接的 Microsoft ActiveX 控件和范例页面。改用 IIS 管理器可使管理更容易，并减少了 IIS 服务器的攻击面。专用 IIS 服务器不需要该组件
服务器端包括	禁用	提供.shtm、.shtml 和.stm 文件的支持。如果在 IIS 服务器中运行的 Web 站点和应用程序都不使用上述扩展的包括文件，请禁用该组件

续表

UI中的组件名称	安装选项	设置逻辑
WebDAV	禁用	WebDAV扩展了HTTP/1.1协议,允许客户端发布、锁定和管理Web中的资源。专用IIS服务器禁用该组件;或使用Web服务扩展禁用该组件
万维网服务	启用	为客户端提供Web服务、静态和动态内容。专用IIS服务器需要该组件

④ 将IIS目录和数据与系统磁盘分开,保存在专用磁盘空间内。

⑤ 在IIS管理器中删除必须之外的任何没有用到的映射(保留ASP等必要映射即可)。

⑥ 在IIS中将HTTP404 Object Not Found出错页面通过URL重定向到一个定制HTM文件。

⑦ Web站点权限设定(建议)如表3-9-4所示。

表3-9-4 Web站点权限设定

Web站点权限	授予的权限	Web站点权限	授予的权限
读	允许	日志访问	建议关闭
写	不允许	索引资源	建议关闭
脚本源访问	不允许	执行	推荐选择"仅限于脚本"
目录浏览	建议关闭		

建议使用W3C扩充日志文件格式,每天记录客户IP地址、用户名、服务器端口、方法、URI字根、HTTP状态和用户代理,而且每天均要审查日志。(最好不要使用默认的目录,建议更换一个记日志的路径,同时设置日志的访问权限,只允许管理员和system为Full Control。)

⑧ 程序安全。涉及用户名与口令的程序最好封装在服务器端,尽量少地出现在ASP文件中,涉及与数据库连接的用户名与口令应给予最小的权限;需要经过验证的ASP页面可跟踪上一个页面的文件名,只有从上一页面转进来的会话才能读取这个页面;防止ASP主页.inc文件泄露问题;防止UE等编辑器生成some.asp.bak文件泄露问题。

(3) 安全更新。

应用所需要的所有Service Pack和定期手动更新补丁。

(4) 安装和配置防病毒保护。

(5) 安装和配置防火墙保护。

(6) 监视解决方案。

根据要求安装和配置MOM代理或类似的监视解决方案。

(7) 加强数据备份。

Web数据定时做备份,保证在出现问题后可以恢复到最近的状态。

(8) 考虑实施IPSec筛选器。

用IPSec过滤器阻断端口。Internet协议安全性(IPSec)过滤器可为增强服务器所需

要的安全级别提供有效的方法。推荐在高安全性环境中使用该选项，以便进一步减少服务器的受攻击面。

有关使用 IPSec 过滤器的详细信息，请参阅模块其他成员服务器强化过程。表 3-9-5 列出在高级安全性环境下可在 IIS 服务器上创建的所有 IPSec 过滤器。

表 3-9-5 IPSec 过滤器设置

服　务	协议	源端口	目标端口	源地址	目标地址	操作	镜像
Terminal Services	TCP	所有	3389	所有	ME	允许	是
HTTP Server	TCP	所有	80	所有	ME	允许	是

3.9.8 实验思考

（1）Internet 服务器的安全加固要从哪些方面考虑？
（2）怎样拒绝 ASP 木马？

3.10 网络安全程序设计

3.10.1 实验类型

设计型，8 学时，课外自选实验。

3.10.2 实验目的

掌握简单的网络安全程序设计方法。

3.10.3 题目描述

使用 Window Raw Socket 技术实现端口扫描和 Web 服务的 CGI 漏洞扫描。

3.10.4 实验要求

理解 Window Raw Socket 技术特点和端口扫描技术的原理，编程实现端口扫描和 CGI 漏洞扫描。

3.10.5 相关知识

从理论上说，任何一门语言都可以在任何一个系统上编程，只要找到该系统提供的

"接口"和对系统内部机制有深入的了解就可以了。正如C语言可以在Windows下编程，也同样可以在Linux上大放异彩一样。

编程是一项很繁杂的工作，除了应用编程工具之外，了解系统本身内部工作机理非常重要，这是写出稳定兼容的程序所必不可少的前提条件。要在哪一种系统上编程，就要对该系统的机制进行研究，至少应该知道一个程序在那个系统上是如何运行的。

1. 了解 Windows 内部机制

Windows 是一个"基于事件的、消息驱动的"操作系统。

在 Windows 下执行一个程序，只要用户进行了影响窗口的动作(如改变窗口大小或移动、单击等)，该动作就会触发一个相应的"事件"。系统每次检测到一个事件时，就会给程序发送一个"消息"，从而使程序可以处理该事件。每个 Windows 应用程序都是基于事件和消息的，而且包含一个主事件循环，它不停地、反复地检测是否有用户事件发生。每次检测到一个用户事件，程序就对该事件做出响应，处理完再等待下一个事件的发生。

Windows 下的应用程序不断地重复这一过程，直至用户终止程序，用代码来描述实际上也就是一个消息处理过程的 while 循环语句。

2. 编程语言以及工具的选择

上面的介绍使我们对 Windows 有了进一步的了解，现在就该开始行动了，选择要学的语言和工具是第一步，而且是非常重要的一步工作，建议一切以简单、易接受为原则，不然会自信心大减的。

3.10.6 实验设备

主流配置 PC，Windows 操作系统，网络环境，Visual Studio 开发平台。

3.10.7 实验步骤

实验内容一：端口扫描器实现

一个扫描器通常由以下三部分组成。

1. 侦听线程

侦听线程负责对扫描的主机返回的数据包进行侦听，并进行分析，得出扫描结果。

```
DWORD WINAPI ListeningFunc(LPVOID lpvoid)
{
//首先建立一个原始套接字
SOCKET rawsock=socket(AF_INET,SOCK_RAW,IPPROTO_IP);
//然后取得本机的 IP地址,确定一个端口绑定原始套接字
struct hostent * pHostent;
char name[100]={0};
```

```
gethostname(name,100);
pHostent=gethostbyname(name);
//把本机 IP 地址复制到 addr_in.sin_addr.S_un.S_addr 中
memcpy(&addr_in.sin_adddr.S_un.S_addr,pHostent->h_addr_list[0],pHostent->h_length);
//绑定
int ret=bind(rawsock,(struct sockaddr *)&addr_in,sizeof(addr_in));
//设置 SIO_RCVALL:接收所有数据包
DWORD lpvBuffer=1;
DWORD lpcbBytesReturned=0;
WSAIoctl(rawsock,SIO_RCVALL,&lpvBuffer,sizeof(lpvBuffer),NULL,0,&lpcbBytesReturned,NULL,NULL);
/*接下来,使用一个死循环来不断地捕获接收到的数据包,分析如果是存活的端口返回的包就打
印出来,不是则放弃,继续捕获下一个包*/
while(TRUE)
{
SOCKADDR_IN from={0};
int size=sizeof(from);
char RecvBuf[256]={0};
//接收数据包
ret=recvfrom(rawsock,RecvBuf,sizeof(RecvBuf),0,(struct sockadddr *)&from,&size);char * sourceip=
inet_ntoa(*(struct in_addr *)&from.sin_addr);if(ret!=SOCKET_ERROR)
{
//分析数据包
IPHEADER * lpIPheader;
lpIPheader=(IPHEADER*)RecvBuf;
if(lpIPheader->proto==IPPROTO_TCP)
{
TCPHEADER * lpTCPheader=(TCPHEADER*)(RecvBuf+sizeof(IPHEADER));
//判断是不是远程开放端口返回的数据包
if(lpTCPheader->th_seq!=0 && lpTCPheader->th_flag==0x12)
{
//如果是,就从 TCP 头中取出端口信息,打印出来
printf("===%s:%d\n",sourceip,ntohs(lpTCPHeader->th_sport));
}
}
}
}//end while
}
```

IPHEADER 和 TCPHEADER 结构定义如下:

```
typedef struct ip_head
{
unsigned char h_verlen;          //4位首部长度,4位 IP版本号
unsigned char tos;               //8位服务类型 TOS
unsigned short total_len;        //16位总长度(字节)
unsigned short ident;            //16位标识
unsigned short frag_and_flags;   //3位标志位(如 SYN、ACK等)
```

```
unsigned char ttl;              //8位生存时间 TTL
unsigned char proto;            //8位协议(如 ICMP、TCP等)
unsigned short checksum;        //16位 IP首部校验和
unsigned int sourceIP;          //32位源 IP地址
unsigned int destIP;            //32位目的 IP地址
}IPHEADER;
typedef struct tcp_header
{
USHORT th_sport;                //16位源端口
USHORT th_dport;                //16位目的端口
unsigned int th_seq;            //32位序列号
unsigned int th_ack;            //32位确认号
unsigned char th_lenres;        //4位首部长度/6位保留字
unsigned char th_flag;          //6位标志位
USHORT th_win;                  //16位窗口大小
USHORT th_sum;                  //16位校验和
USHORT th_urp;                  //16位紧急数据偏移量
}TCPHEADER;
```

2. 发包线程

如何构造 SYN 包来进行发送是发包程序的内容,有两种方法:一种方法是自己构造 IP 头和 TCP 头,然后自己计算校验和;另一种方法是采用 connect()函数调用,这个调用就隐含了 TCP 三次握手,在第一次握手时关闭连接,这样也能发送 SYN 包。这里采取第二种方法,并设置套接字为非阻塞类型。

```
DWORD WINAPI scan(LPVOID lp)
{
SOCKET sock=NULL;
SOCKADDR_IN addr_in={0};
TCHAR SendBuf[256]={0};
INFO * lpInfo=(INFO * )lp;
int iErr;
ULONG ul=1;
USHORT port=lpInfo->port;
addr_in.sin_family=AF_INET;
addr_in.sin_port=htons(port);
addr_in.sin_addr.S_un.S_addr=lpInfo->IP;
if((sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP))==INVALID_SOCKET)
printf("socket setup error!\n");
iErr=ioctlsocket(sock,FIOBIO,(unsigned long * )&ul);  //设置 sock为非阻塞
connect(sock,(struct sockaddr * )&addr_in,sizeof(addr_in));      //发送 SYN包
closesocket(sock);
return 0;
}
```

INFO为自定义的一个结构,用于存储扫描目标地址和端口号,定义如下:

```
typedef struct info
{
ULONG IP;
USHORT port;
}INFO;
```

3. 主程序

主程序主要完成从命令行中提取IP地址和端口然后调用发送函数。

```
int main(int argc,char * argv[])
{
WSADATA WSAData;
INFO info={0};
ULONG StartIP=0,EndIP=0;
int number=0;
if(WSAStartup(MAKEWORD(2,2),&WSAData)!=0)
{
printf("int WSAStartup Error!\n");
return 0;
}
//创建一个侦听线程来分析接收到的包
CreateThread(NULL,0,ListeningFunc,&tempnum,NULL,NULL);
Sleep(500);                           //等待线程的初始化完成
StartIP=ntohl(inet_addr(argv[1]));
EndIP=ntohl(inet_addr(argv[2]));
for(;StartIP<=EndIP;StartIP++)        //从第一个 IP 到最后一个 IP
{
info.IP=htonl(StartIP);
int Num=ListNum;                      //ListNum为定义的端口列表的长度
while(Num--)
{
info.port=PortList[Num];              //从列表中取出端口值
scan(&info);                          //对目标 IP、端口发送 SYN 包
} //end while
} //end for
Sleep(2000);                          //等待两秒,等最后发出的包返回
printf("Scan Complete!\n");
return 1;
}
```

实验内容二:CGI漏洞扫描器

1. 介绍

漏洞扫描需要针对一定的服务来进行。本例对Web服务器进行CGI漏洞扫描。

2. 原理

CGI扫描需要和被扫描的主机的80端口(就是Web服务器运行的端口号)建立连接,然后提交GET请求,再根据返回的信息加以判断。如果返回200表示成功,返回404表示无法找到指定的文件,返回403表示文件不可用。返回的数据形式为"HTTP/1.1 200"这样的字符串。

3. 实现主程序

```
int main(int argc,char * argv[])
{
WSADATA WSAData;
FILE * fp=NULL;
//打开漏洞列表文件,文件的内容为"GET/_vti_bin/shtml.ext"等 CGI 指令
fp=fopen("cgi.lst","r");
INFO info={0};
if(argc!=2)return 0;
memcpy(info.IP,argv[1],strlen(argv[1]));
printf("Scan Start....\n");
//从文件中读出要扫描的 CGI 信息
while(fgets(info.sendbuf,100,fp)!=NULL)
{
HANDLE h=0;
h=CreateThread(NULL,0,scan,&info,NULL,NULL);      //创建一个线程扫描
if(h==NULL)printf("Create Thread Error!\n");
WaitForSingleObject(h,INFINITE);                  //等待一次扫描结果
memset(info.sendBuf,0,100);
}
printf("Scan Complete!\n");
}
```

INFOR结构用来传递CGI指令和IP信息:

```
typedef struct
{
char sendBuf[100];
char IP[20];
}INFOR
```

4. 扫描线程

```
DWORD WINAPI scan(LPVOID lp)
{
SOCKET sock=NULL;
SOCKADDR_IN target={0};
int error=0;
char buf[256]={0};
```

```
char * p=NULL;
INFOR * lpInfo= (INFOR * )lp;
if((sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP))==INVALID_SOCKET)
{
printf("Socket Setup Error");
return FALSE;
}
target.sin_family=AF_INET;target.sin_port=
htons(80);target.sin_addr.S_un.S_addr=
inet_addr(lpInfo->IP);
error=connect(sock,(struct sockaddr * )&target,sizeof(target));        //连接
if(error==SOCKET_ERROR)
{
printf("Connect Error!\n");
return FALSE;
}
send(sock,lpInfo->sendBuf,100,0);                    //发送 GET 请求
recv(sock,buf,256,0);                                //接收返回的信息
p=strstr(buf,"HTTP/1.1 200");                        //判断请求是否成功
if(p!=NULL)
{
//包含"HTTP/1.1 200"字符串,则表示有相应的漏洞
printf("%s",lpInfo->sendBuf);                        //打印出相应的漏洞
}
closesocket(sock);
return 1;
}
```

3.10.8 实验思考

1. 端口扫描的方法有哪些?
2. ASP 网站的安全扫描是怎样进行的?

3.11 应用程序保护

3.11.1 实验类型

设计型,4 学时,课外自选实验。

3.11.2 实验目的

通过实验,使学生了解应用程序完整性鉴别的方法、注册方法等。

3.11.3 题目描述

使用 WinMD5 生成散列值保护程序的完整性，应用程序加壳，程序注册。

3.11.4 实验要求

理解应用程序保护的作用，能够使用文件散列值判断程序的完整性，理解应用程序加壳的原理。

提高要求：设计实现一种应用程序加壳的方法和程序注册的方法。

3.11.5 相关知识

WinMD5 是一款对所有文件 MD5 值检测的软件。MD5 的实际应用是对一段 Message(字节串)产生 fingerprint(指纹)，可以防止被"篡改"，其广泛用于加密和解密技术上。该软件使用极其简单，运行后，把需要计算 MD5 值的文件用鼠标拖到正在处理的框里边，下面将直接显示其 MD5 值以及所测试的文件名称，可以保留多个文件测试的 MD5 值，选定所需要复制的 MD5 值，用 Ctrl+C 组合键就可以复制到其他地方了。

3.11.6 实验设备

主流配置 PC 一台，Windows 操作系统。

3.11.7 实验步骤

实验内容一：WinMD5 使用

(1) 打开文件 WinMD5.exe，如图 3-11-1 所示。

(2) 拖动需要验证的文件到此工具界面里，等待生成 MD5 串，如图 3-11-2 所示。



图 3-11-1 WinMD5.exe

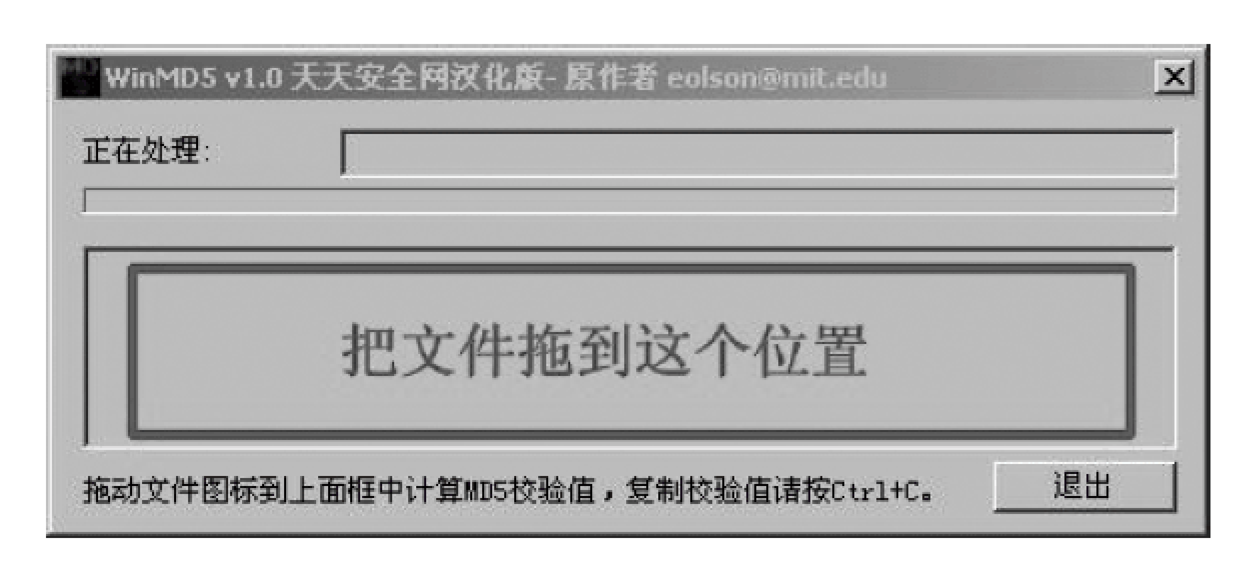


图 3-11-2 操作演示

(3) 比较 MD5 串是否一样，如图 3-11-3 所示。



图 3-11-3　比较

(4) 如果正确，说明下载完整；如果不正确，说明文件已经破坏，请重新下载或不使用此文件。

实验内容二：应用程序的注册及破解

(1) 使用 MS VB 6.0 编写一个简单的注册程序，输入正确的注册信息后才能显示一段信息。

(2) 使用追踪调试工具进行注册程序的跟踪，并修改跳转条件部分，使得不需要输入注册信息仍能显示这段信息。

3.11.8　实验思考

(1) 应用程序加壳的原理是怎样的？

(2) 木马病毒免杀从哪些方面来考虑？

3.12　网络监控与协议分析

3.12.1　实验类型

综合型，4 学时，必选实验。

3.12.2　实验目的

能够对当前的网络流量、协议分布等状态做出正确判断；能够对网络协议的工作过程做出正确的分析。

3.12.3 题目描述

使用数据嗅探软件 Sniffer 进行协议分析与密码捕获。

3.12.4 实验要求

理解交换环境与共享式网络环境进行数据嗅探的区别，能够使用数据嗅探软件进行协议分析和密码捕获。

3.12.5 相关知识

嗅探器的英文写法是 Sniff，可以理解为一个安装在计算机上的窃听设备，它可以用来窃听计算机在网络上所产生的众多的信息。简单一点解释：一部电话的窃听装置可以用来窃听双方通话的内容，而计算机网络嗅探器则可以窃听计算机程序在网络上发送和接收到的数据。

可是，计算机直接传送的数据是大量的二进制数据，因此，一个网络窃听程序必须使用特定的网络协议来分解嗅探到的数据，嗅探器也必须能够识别出哪个协议对应于这个数据片断，只有这样才能够进行正确的解码。

计算机的嗅探器比起电话窃听器，有它独特的优势：很多的计算机网络采用的是"共享媒体"，也就是说，不必中断它的通信，并且配置特别的线路，再安装嗅探器，几乎可以在任何连接着的网络上直接窃听到同一掩码范围内的计算机网络数据，称这种窃听方式为"基于混杂模式的嗅探"(promiscuous mode)。尽管如此，这种"共享"的技术发展的很快，慢慢转向"交换"技术，这种技术会长期地继续使用下去，它可以实现有目的选择的收发数据。

3.12.6 实验设备

主流配置 PC 一台，Windows 2003 操作系统，共享式局域网环境，Wireshark。

3.12.7 实验步骤

(1) 在 Windows 下安装 Wireshark 工具，过程如图 3-12-1、图 3-12-2 所示。

(2) 测试一下网络环境是否能 ping 通，如图 3-12-3 所示。



图 3-12-1 Wireshark 安装一

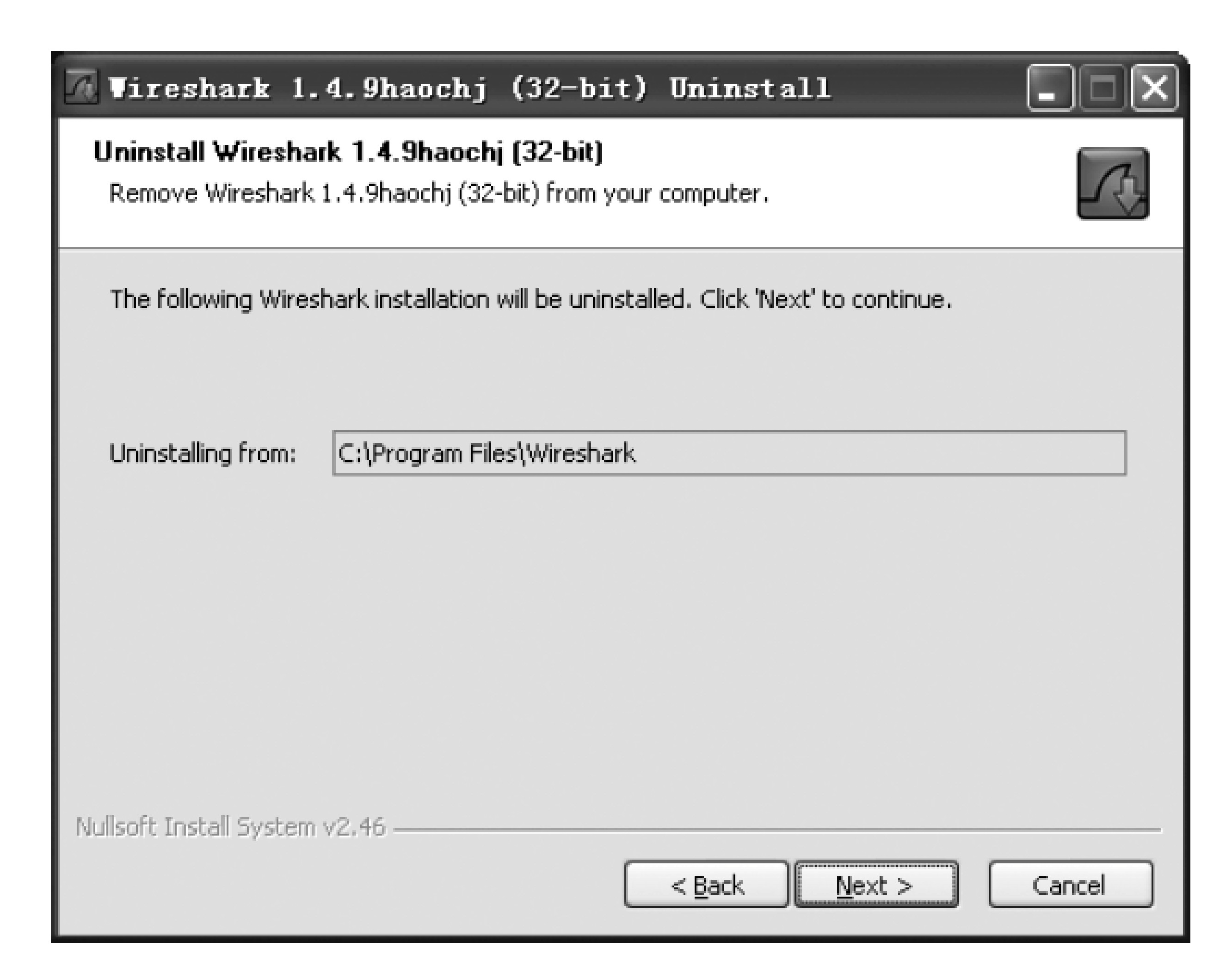


图 3-12-2 Wireshark 安装二

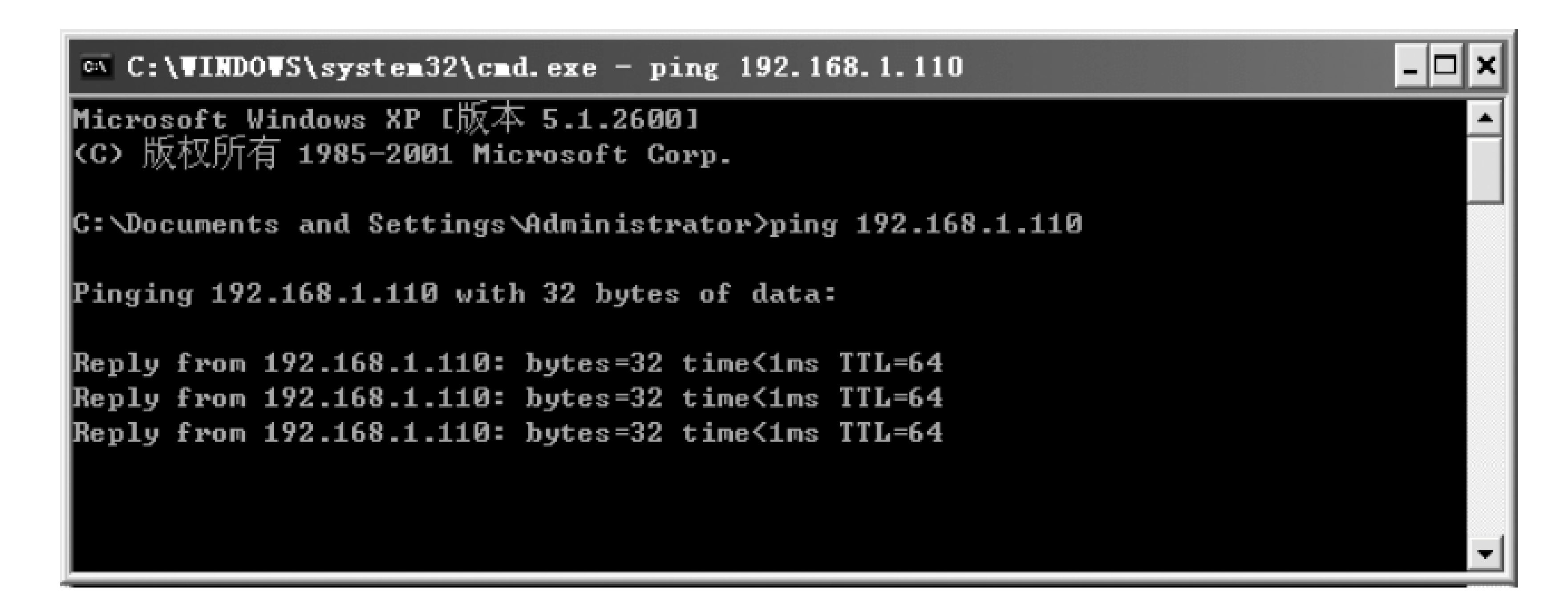


图 3-12-3 ping 网络

（3）启动监听，选择抓包过滤，新建一个过滤类型ICMP，如图3-12-4所示。

Wireshark:抓包文件 - 配置文件:Default
编辑
新建(N)
删除(D)
抓包过滤器
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
No Broadcast and no Multicast
No ARP
IP only
IP address 192.168.0.1
IPX only
TCP only
UDP only
TCP or UDP port 80 (HTTP)
HTTP TCP port (80)
No ARP and no DNS
Non-HTTP and non-SMTP to/from www.wireshark.org
ICMP
属性
过滤名字: ICMP
过滤条件: icmp
帮助(H)
确定(O)
取消(C)

图3-12-4　新建过滤文件

（4）执行ping扫描，如图3-12-5所示。

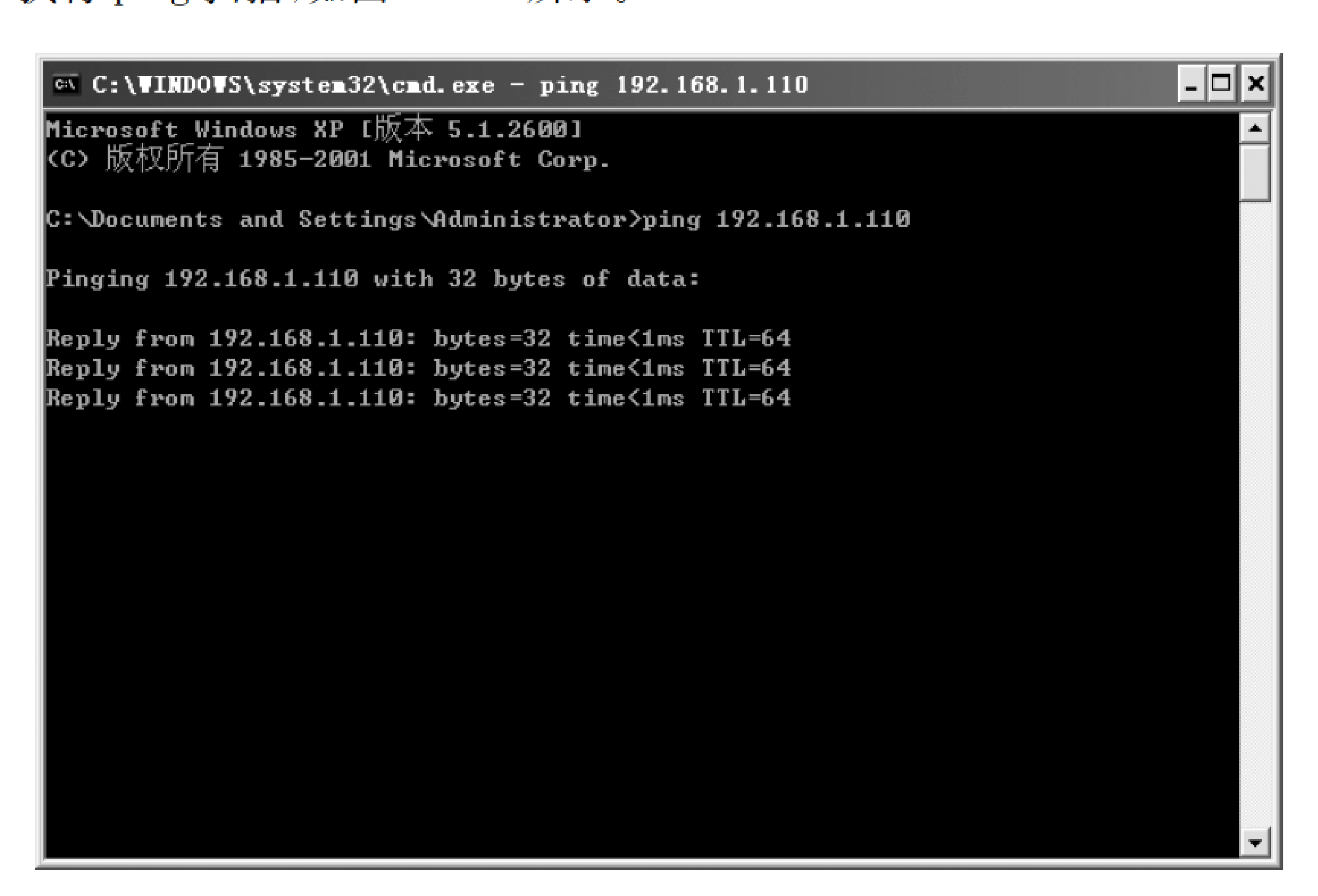


图3-12-5　ping扫描

（5）停止监听，查看监听结果，如图3-12-6所示。

（6）用Wireshark监听FTP账户/密码，新建一个用户账号及密码，过程如图3-12-7～图3-12-12所示。

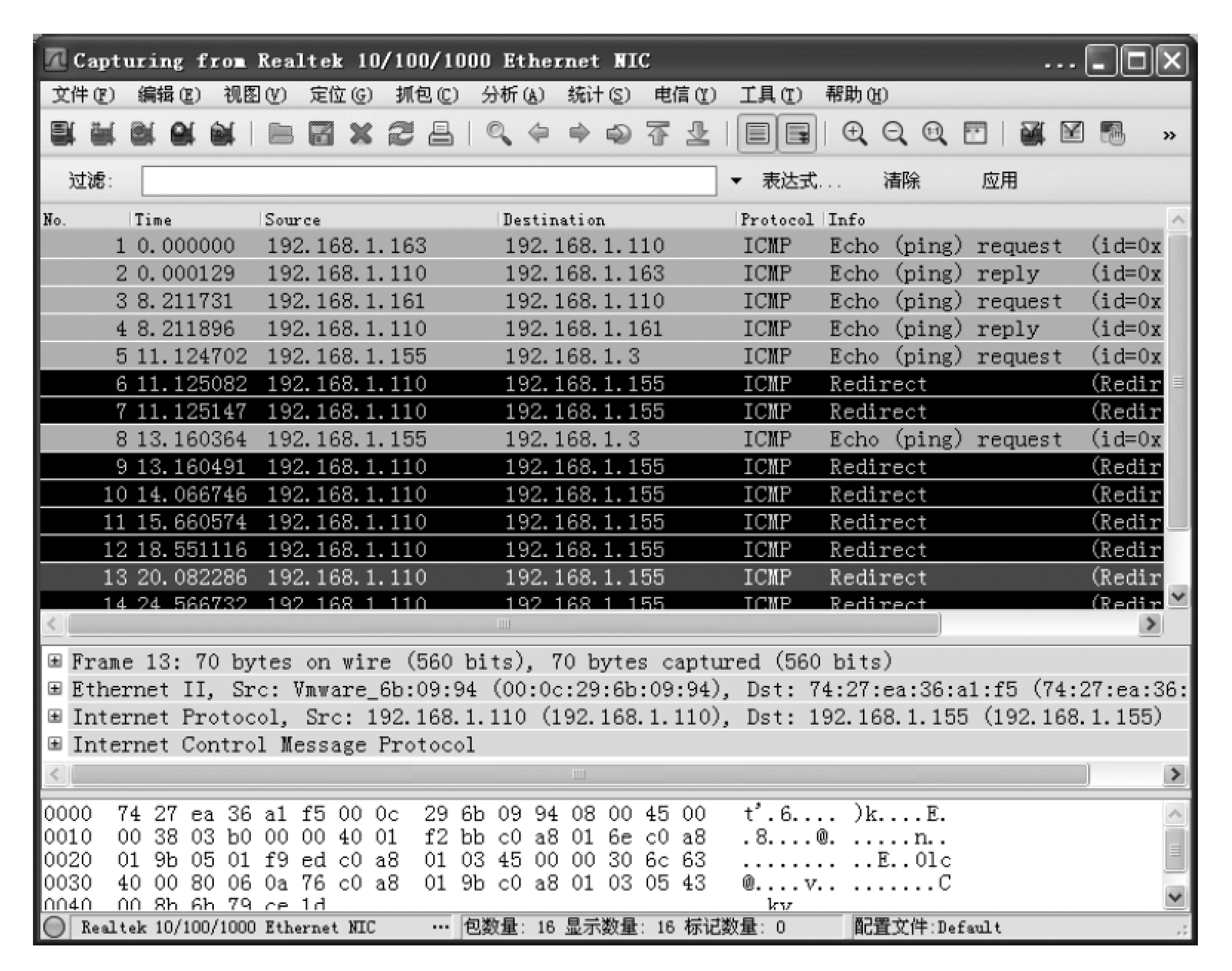


图 3-12-6 监听结果

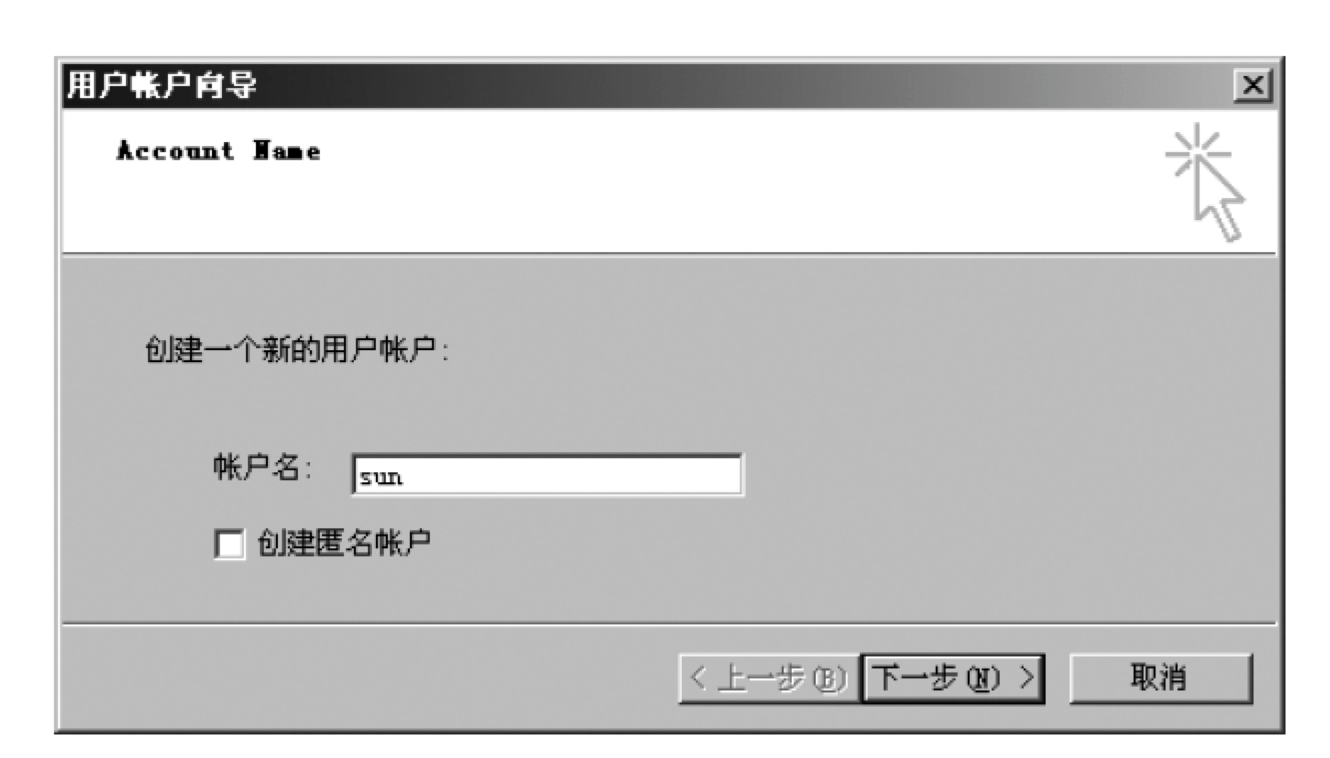


图 3-12-7 新建步骤一



图 3-12-8 新建步骤二

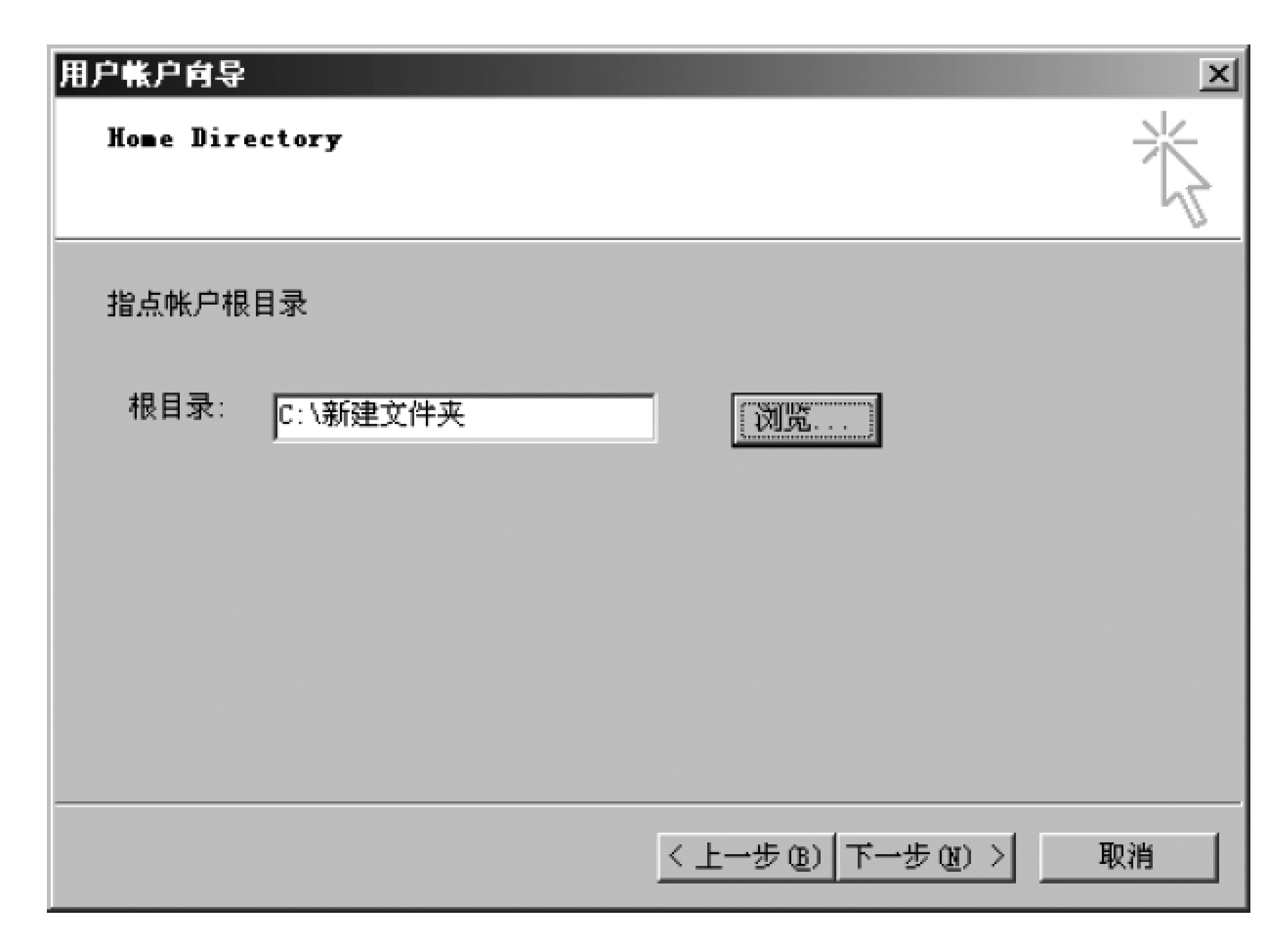


图 3-12-9　新建步骤三

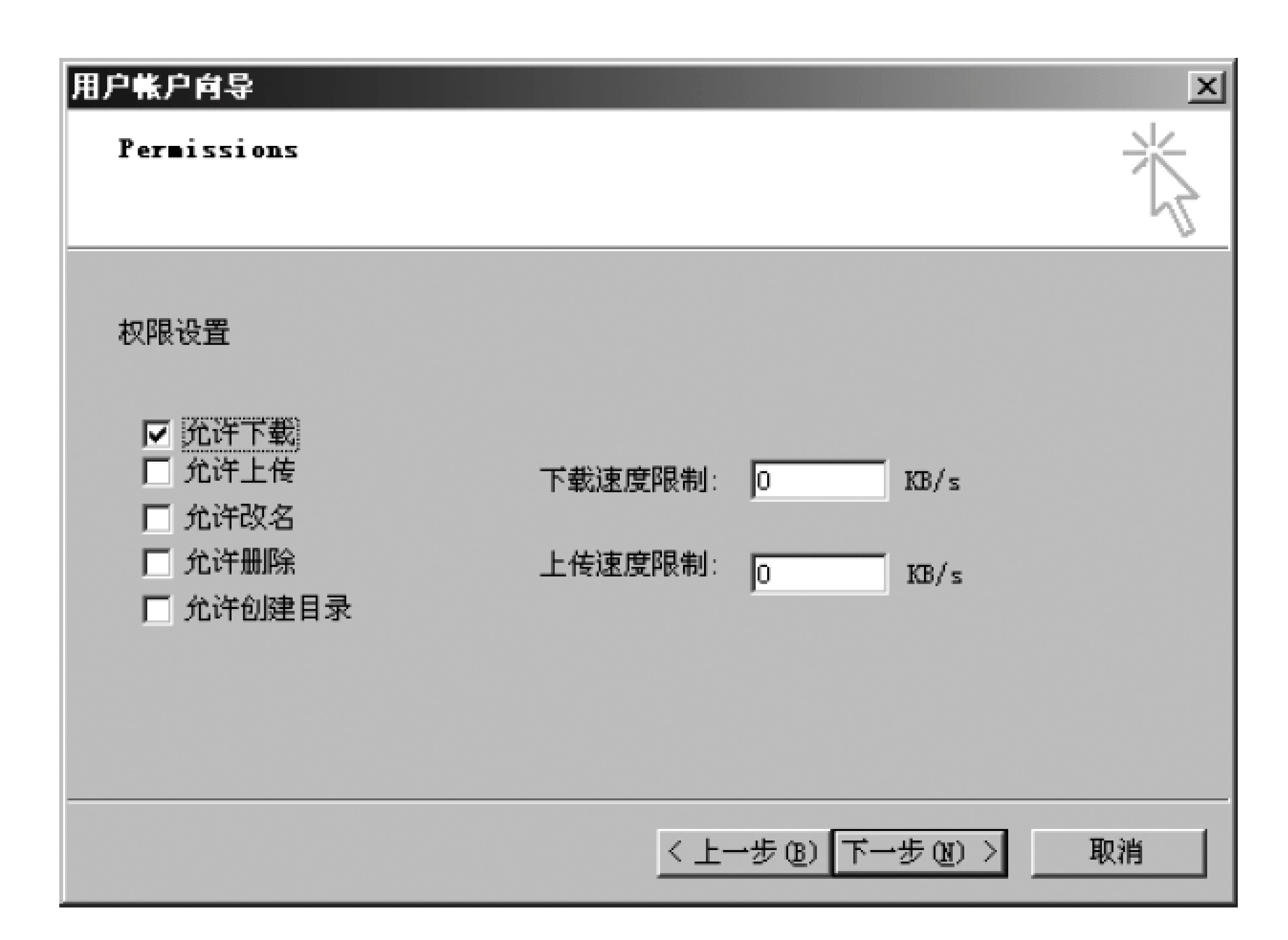


图 3-12-10　新建步骤四

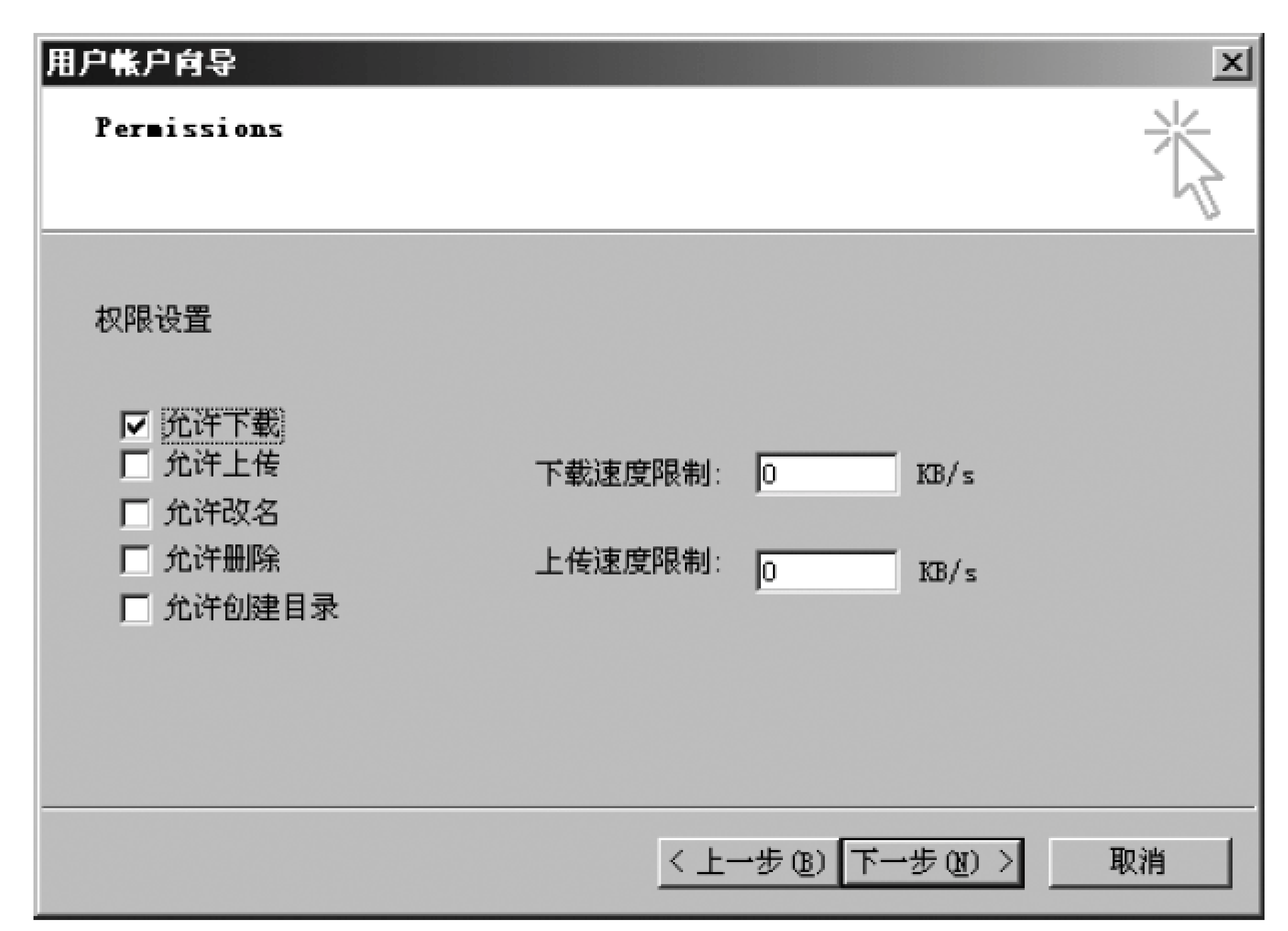


图 3-12-11　新建步骤五



图 3-12-12　新建步骤六

(7) 启动服务器，如图 3-12-13 所示。



图 3-12-13　启动服务器

(8) 打开浏览器，登录服务器，弹出如图 3-12-14 所示对话框，输入用户名及密码登录服务器。

(9) 登录服务器成功，如图 3-12-15 所示。

(10) 停止抓包，查看结果，如图 3-12-16 和图 3-12-17 所示。

3.12.8　实验思考

(1) 在交换式局域网环境和共享式局域网环境中进行网络嗅探有何不同？

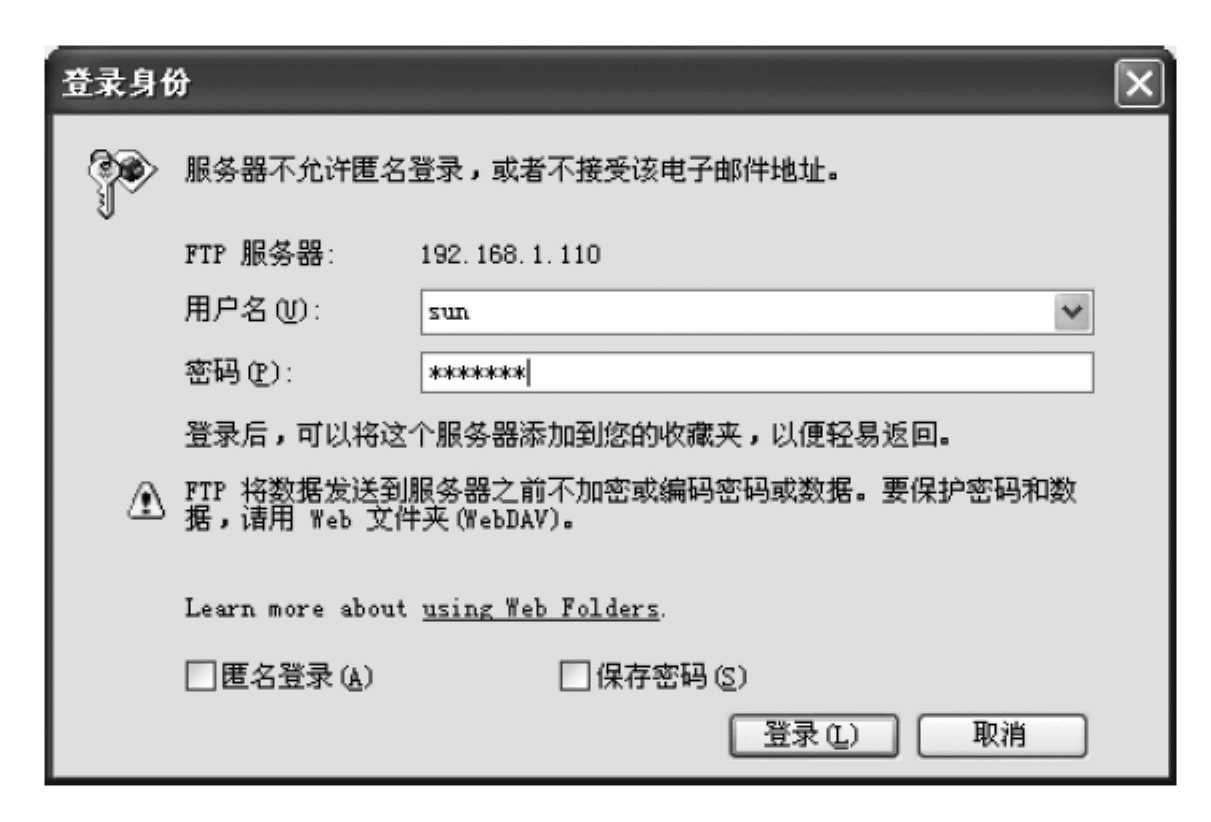


图 3-12-14　登录对话框

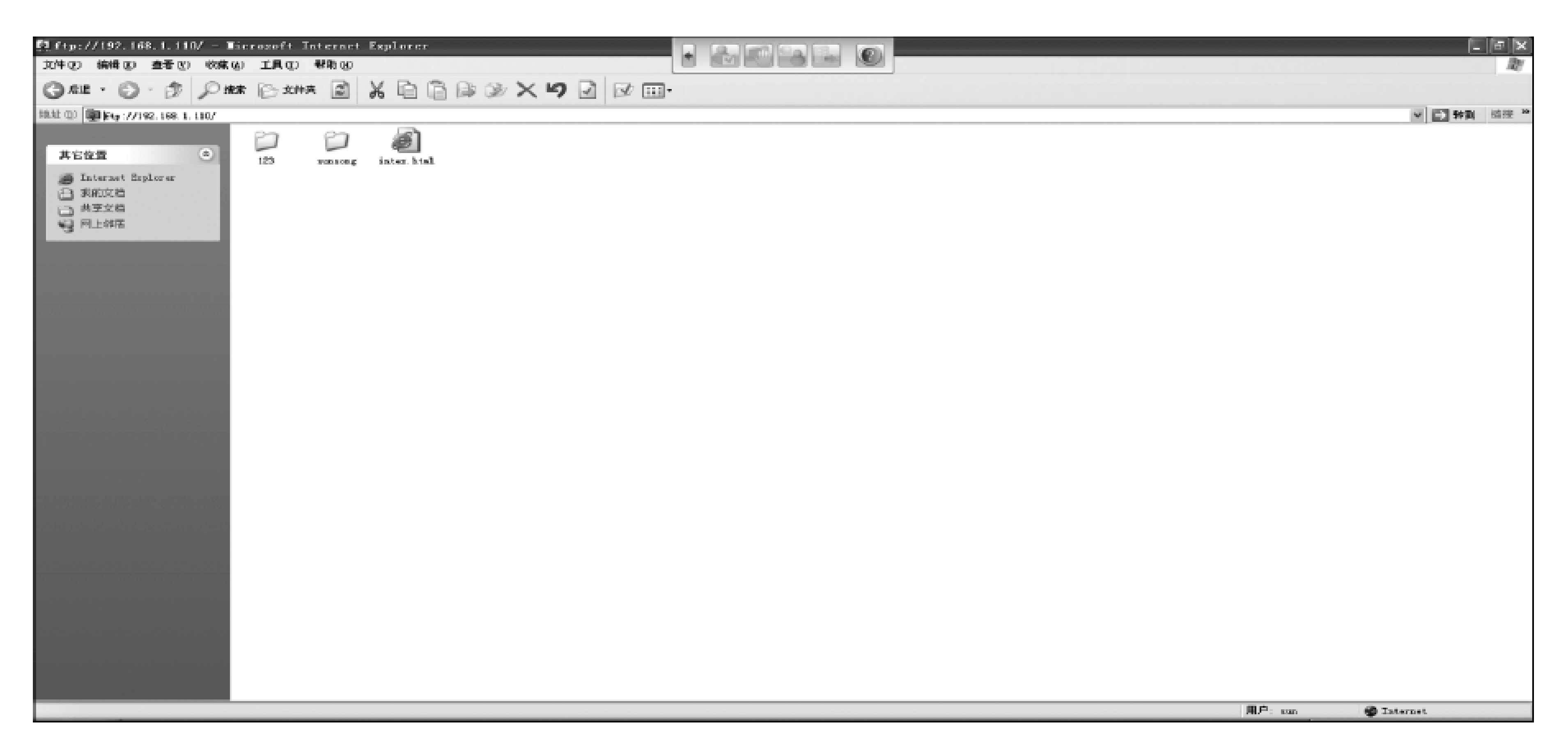


图 3-12-15　登录成功

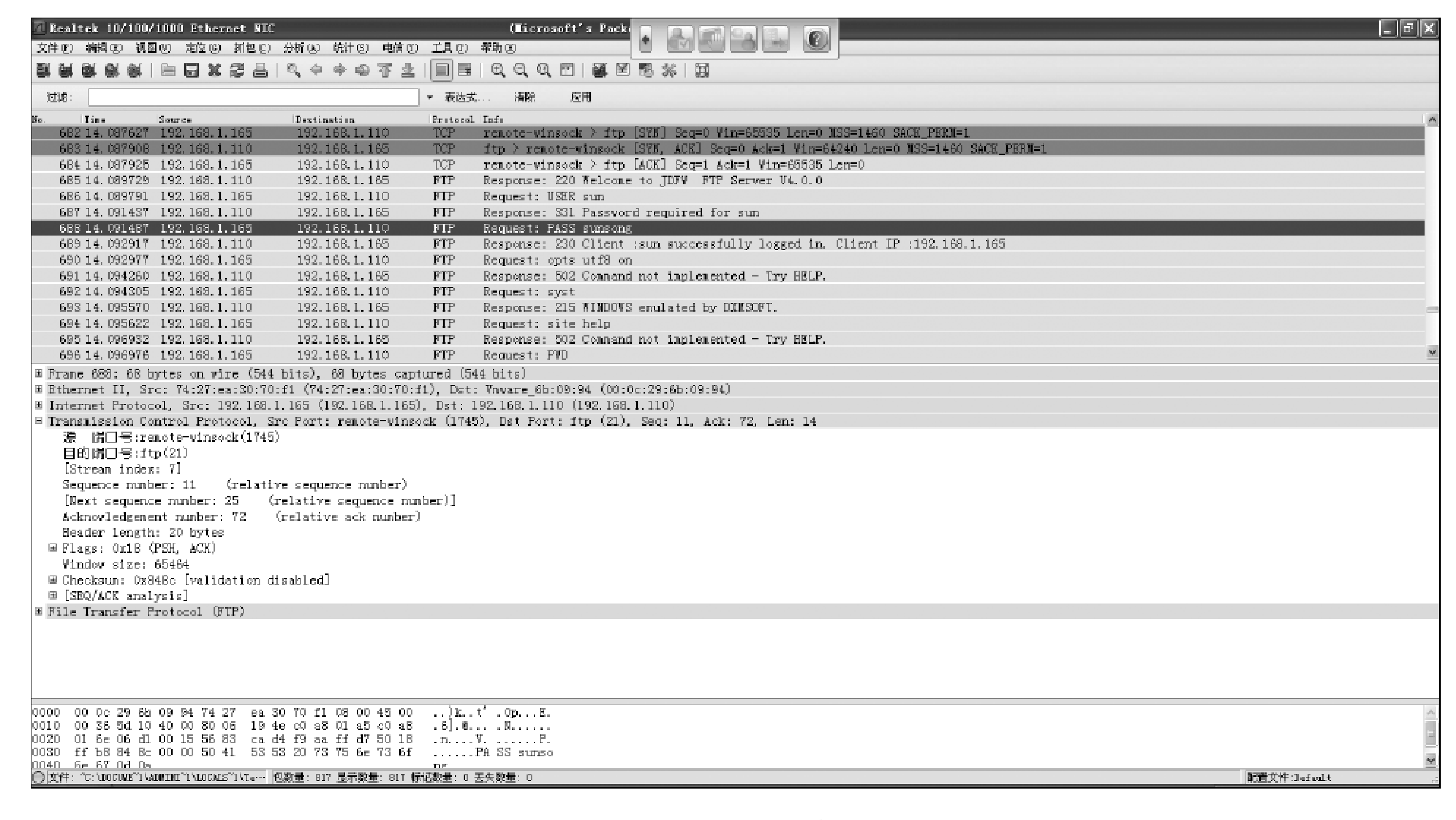


图 3-12-16　查看结果一

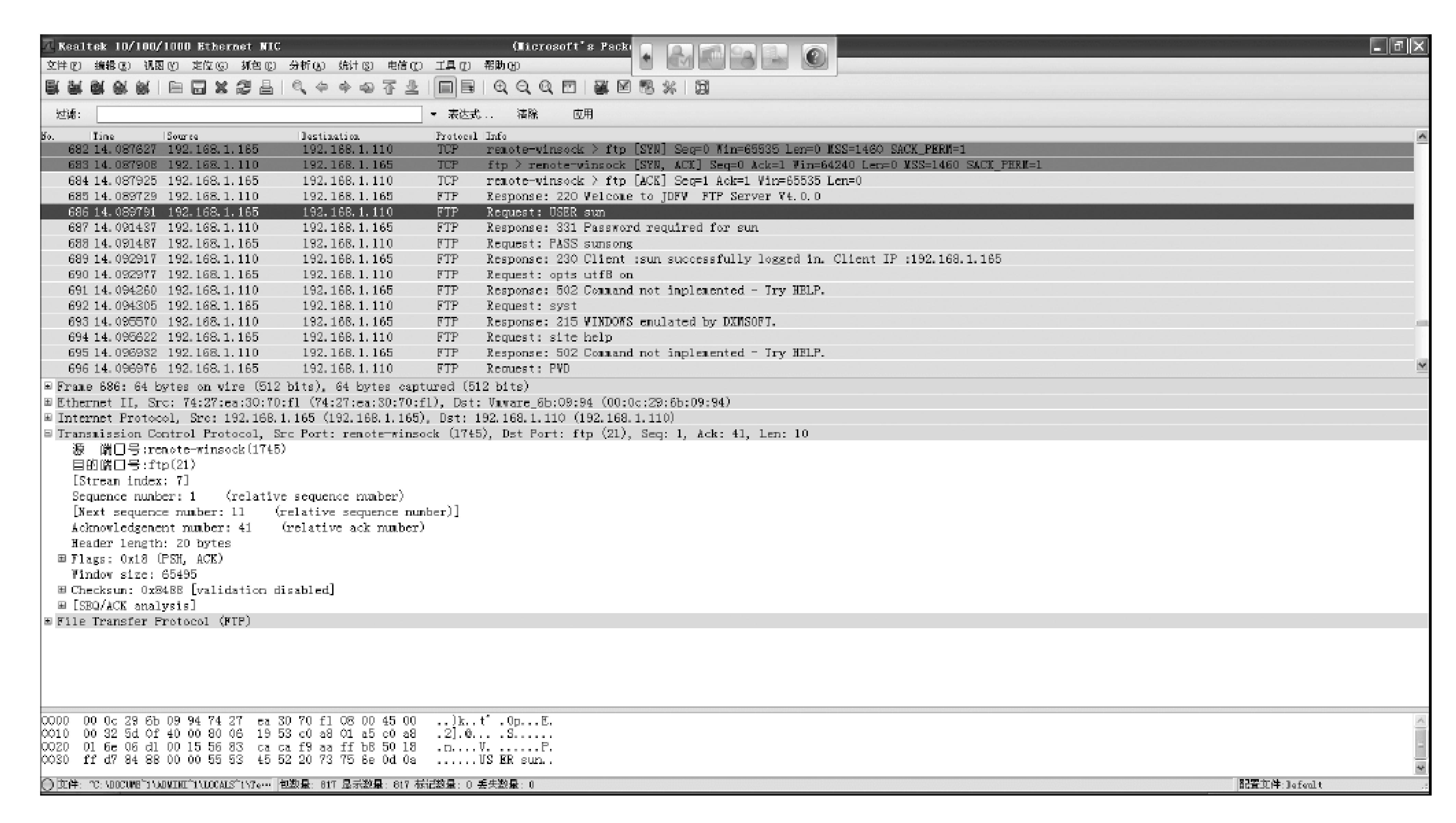


图 3-12-17　查看结果二

（2）有哪些方法可以使网络嗅探失败？

3.13　风险分析

3.13.1　实验类型

设计型，2 学时，课外自选实验。

3.13.2　实验目的

了解风险评估、风险减缓的步骤和基本内容。

3.13.3　题目描述

使用数据恢复软件 EasyRecovery 进行文件恢复。

3.13.4　实验要求

理解磁盘数据恢复的原理，认识数据恢复技术对信息安全的影响；能够使用数据恢复软件 EasyRecovery 进行文件恢复。

提高要求：能够对磁盘数据进行彻底清除。

3.13.5 相关知识

随着 Internet 的急剧扩大和上网用户的迅速增加,风险变得更加严重和复杂。原来由单个计算机安全事故引起的损害可能传播到其他系统,引起大范围的瘫痪和损失;加上缺乏安全控制机制和对 Internet 安全政策的认识不足,这些风险正日益严重。

针对这个企业局域网中存在的安全隐患,在进行安全方案设计时,下述安全风险必须认真考虑,并且要针对面临的风险,采取相应的安全措施。下述风险由多种因素引起,与这个企业局域网结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。

网络安全可以从以下 5 个方面来理解:①网络物理是否安全;②网络平台是否安全;③系统是否安全;④应用是否安全;⑤管理是否安全。针对每一类安全风险,结合这个企业局域网的实际情况,我们将具体地分析网络的安全风险。

1. 物理安全风险分析

网络的物理安全的风险是多种多样的。网络的物理安全主要是指地震、水灾、火灾等环境事故,电源故障,人为操作失误或错误,设备被盗、被毁,电磁干扰,线路截获,以及高可用性的硬件,双机多冗余的设计,机房环境及报警系统,安全意识等。它是整个网络系统安全的前提,在这个企业局域网内,由于网络的物理跨度不大,只要制订健全的安全管理制度,做好备份,并且加强网络设备和机房的管理,这些风险是可以避免的。

2. 网络平台的安全风险分析

网络结构的安全涉及网络拓扑结构、网络路由状况及网络的环境等。

1) 公开服务器面临的威胁

这个企业局域网内公开服务器区(WWW、E-mail 等服务器)作为公司的信息发布平台,一旦不能运行或者受到攻击,将对企业的声誉造成巨大影响。同时,公开服务器本身要为外界服务,必须开放相应的服务;每天,黑客都在试图闯入 Internet 节点,这些节点如果不保持警惕,可能连黑客怎么闯入的都不知道,甚至会成为黑客入侵其他站点的跳板。因此,规模比较大的网络的管理人员对 Internet 安全事故做出有效反应变得十分重要。我们有必要将公开服务器、内部网络与外部网络进行隔离,避免网络结构信息外泄;同时还要对外网的服务请求加以过滤,只允许正常通信的数据包到达相应主机,其他的请求服务在到达主机之前就应该遭到拒绝。

2) 整个网络结构和路由状况

安全的应用往往是建立在网络系统之上的。网络系统的成熟与否直接影响安全系统的建设。在这个企业局域网络系统中,只使用了一台路由器,用作与 Internet 连接的边界路由器,网络结构相对简单,具体配置时可以考虑使用静态路由,这就大大地减少了因网络结构和网络路由造成的安全风险。

3. 系统的安全风险分析

所谓系统的安全,是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任。对于中国来说,恐怕没有绝对安全的操作系统可以选择,无论是 Microsoft 的 Windows NT 或者其他任何商用 UNIX 操作系统,其开发厂商必然有其 Back-Door。但是,我们可以对现有的操作平台进行安全配置,对操作和访问权限进行严格控制,提高系统的安全性。因此,不但要选用尽可能可靠的操作系统和硬件平台,而且必须加强登录过程的认证(特别是在到达服务器主机之前的认证),确保用户的合法性;其次应该严格限制登录者的操作权限,将其完成的操作限制在最小的范围内。

4. 应用的安全风险分析

应用系统的安全跟具体的应用有关,它涉及很多方面。应用系统的安全是动态的、不断变化的。应用的安全涉及面很广,以目前 Internet 上应用最为广泛的 E-mail 系统来说,其解决方案有几十种,但其系统内部的编码甚至编译器导致的 Bug 是很少有人能够发现的,因此一套详尽的测试软件是必需的。但是应用系统是不断发展且应用类型是不断增加的,其结果是安全漏洞也在不断增加且隐藏得越来越深。因此,保证应用系统的安全也是一个随网络发展不断完善的过程。

应用的安全性涉及信息、数据的安全性。信息的安全性涉及机密信息泄露、未经授权的访问、破坏信息完整性、假冒和破坏系统的可用性等。由于这个企业局域网跨度不大,绝大部分重要信息都在内部传递,因此信息的机密性和完整性是可以保证的。对于有些特别重要的信息需要对内部进行保密的(例如领导子网、财务系统传递的重要信息),可以考虑在应用级进行加密;针对具体的应用,直接在应用系统开发时进行加密。

5. 管理的安全风险分析

管理是网络安全中最重要的部分,责权不明、管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。

当网络出现攻击行为或网络受到其他一些安全威胁时(如内部人员的违规操作等),无法进行实时的检测、监控、报告与预警。同时,当事故发生后,也无法提供黑客攻击行为的追踪线索及破案依据,即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录,及时发现非法入侵行为。

建立全新网络安全机制,必须深刻理解网络并能提供直接的解决方案,因此,最可行的做法是管理制度和解决方案的结合。

6. 黑客攻击

黑客的攻击行动是无时无刻不在进行的,而且会利用系统和管理上的一切可能利用的漏洞。公开服务器存在漏洞的一个典型例证,是黑客可以轻易地骗过公开服务器软件,得到 UNIX 的口令文件并将之送回。黑客侵入 UNIX 服务器后,有可能修改特权,从普通用户变为高级用户,一旦成功,黑客可以直接进入口令文件。黑客还能开发欺骗程序,

将其植入 UNIX 服务器中，用以监听登录会话。当它发现有用户登录时，便开始存储一个文件，这样黑客就拥有了他人的账户和口令。这时为了防止黑客入侵，需要设置公开服务器，使得它不离开自己的空间而进入另外的目录。另外，还应设置组特权，不允许任何使用公开服务器的人访问 WWW 页面文件以外的东西。在这个企业的局域网内可以综合采用防火墙技术、Web 页面保护技术、入侵检测技术和安全评估技术来保护网络内的信息资源，防止黑客攻击。

7. 通用网关接口(CGI)漏洞

有一类风险涉及通用网关接口(CGI)脚本。许多页面文件有指向其他页面或站点的超链接，有些站点用这些超链接所指站点寻找特定信息。搜索引擎是通过 CGI 脚本执行的方式实现的。黑客可以修改这些 CGI 脚本以执行他们的非法任务。通常，这些 CGI 脚本只能在这些 WWW 服务器中寻找，但如果进行一些修改，它们就可以在 WWW 服务器之外进行寻找。要防止这类问题发生，应将这些 CGI 脚本设置为较低级用户特权，提高系统的抗破坏能力，提高服务器的备份与恢复能力，提高站点内容的防篡改与自动修复能力。

8. 恶意代码

恶意代码不限于病毒，还包括蠕虫、特洛伊木马、逻辑炸弹和其他未经同意的软件。应该加强对恶意代码的检测。

9. 病毒的攻击

计算机病毒一直是计算机安全的主要威胁。能在 Internet 上传播的新型病毒，例如通过 E-mail 传播的病毒，增加了这种威胁的程度。病毒的种类和传染方式也在增加，国际空间的病毒总数已达上万甚至更多。当然，查看文档、浏览图像或在 Web 上填表都不用担心病毒感染，然而，下载可执行文件和接收来历不明的 E-mail 文件需要特别警惕，否则很容易导致系统的严重破坏。典型的 CIH 病毒就是一个可怕的例子。

10. 不满的内部员工

不满的内部员工可能在 WWW 站点上开些小玩笑，甚至进行破坏。无论如何，他们最熟悉服务器、小程序、脚本和系统的弱点。对于已经离职的不满员工，可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工，这些员工比已经离开的员工能造成更大的损失，例如他们可以传出至关重要的信息、泄露重要的信息安全、错误地进入数据库、删除数据等。

11. 网络的攻击手段

一般认为，目前对网络的攻击手段主要表现为非授权访问，即没有经过预先同意，就使用网络或计算机资源，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式。

(1) 信息泄露或丢失：指敏感数据在有意或无意中被泄露出去或丢失，它通常包括

信息在传输中丢失或泄露(如黑客们利用电磁泄露或搭线窃听等方式可截获机密信息,或通过对信息流向、流量、通信频度和长度等参数的分析,推出有用信息,如用户口令、账号等重要信息),信息在存储介质中丢失或泄露,通过建立隐蔽隧道等窃取敏感信息等。

(2) 破坏数据完整性:以非法手段窃得对数据的使用权,删除、修改、插入或重发某些重要信息,以取得有益于攻击者的响应;恶意添加、修改数据,以干扰用户的正常使用。

(3) 拒绝服务攻击:它不断对网络服务系统进行干扰,改变其正常的作业流程,执行无关程序,使系统响应减慢甚至瘫痪,影响正常用户的使用,甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

利用网络传播病毒:通过网络传播计算机病毒,其破坏性大大高于单机系统,而且用户很难防范。

3.13.6 实验设备

主流配置PC一台,Windows操作系统。

3.13.7 实验步骤

1. 背景介绍

这是一家商业银行,该银行需要建立门户Web网站,其中涉及的关键业务主要包括:

(1) 用户在线注册;
(2) 用户在线交流;
(3) 在线反馈;
(4) 文件管理。

该网站的主要设备包括:

(1) Web服务器;
(2) 数据库服务器;
(3) E-mail服务器。

由于涉及银行的信誉和利益,该网站要求具有7×24小时服务的能力,并且能抵御基本的攻击,具有从攻击等灾难中恢复的能力。

2. 网络结构设计

考虑业务的需要,设计并实现该网站,价格控制在100万元人民币以内,要求进行概要设计、逻辑设计和物理设计。软件实现上,考虑使用XOOPS+Linux+MySQL来构建。

3. 技术策略

技术策略指对安全防护采取的具体措施和实施的时间。常规防护技术措施有:

(1) 采用备份来避免总体损失;
(2) 帮助用户自助;
(3) 预防引导病毒;
(4) 预防文件病毒;
(5) 将访问控制加到PC中;
(6) 防止无意的信息披露;
(7) 使用服务器安全;
(8) 使用网络操作系统的安全功能;
(9) 阻止局外人攻击;
(10) 不要促成过早的硬件故障;
(11) 为灾难准备硬件;
(12) 学习数据恢复的基本知识,制订技术策略时,要求考虑技术措施以及采取该措施的时机。

4. 应急响应

应急响应指为紧急事件制订响应规划,对不同的网络突发事件作出响应。应急响应的基本过程为:

(1) 事先准备记录重要文件的加密校验和;增加或启用安全审核记录;建立主机的防御能力(补丁、服务、网络配置);备份关键数据(包括防火墙、路由器的配置文件);对用户进行主机安全方面的培训。

(2) 网络的准备工作安装防火墙和入侵检测系统;在路由器上使用访问控制列表;创建有助于监视的网络拓扑结构;对网络流量进行加密;要求认证。

(3) 确定适当的策略和程序:确定响应立场;理解策略;帮助确定调查步骤和方式;制订可接受的使用策略;制订应急响应程序。

(4) 创建响应工具包:响应硬件(PC);响应软件(两到三种本地操作系统、驱动程序、浏览器和备份程序);网络流量监视平台。

(5) 组建应急响应队伍:确定应急响应队伍的任务;应急响应队伍的组建(人数、技术构成);应急响应培训。

5. 安防制度

(1) 介绍。

安防制度通过对操作者使用网络的行为进行规定从而减少安全风险,通常包括资源条例、使用条例、账号条例等。

(2) 举例。

后附文件经下列人员签署并发布实施:

安防执行官:xx 日期:1999年7月8日

首席执行官:yy 日期:1999年7月8日

关于遵守信息安防制度的通知和同意书后附文件是Anson公司的信息安防制度。

我已经认真阅读并理解 Anson 公司的信息安防制度,并且同意遵守它的各项规定。

Anson 公司计算机资源使用条例 签名日期

以下是 Anson 公司计算机资源的使用管理条例。本条例所指的计算机资源包括放置在 Anson 公司的计算机系统与设备以及 Anson 公司/Anson 公司员工/Anson 公司顾客操作使用的计算系统和设备;其中包括但不限于由 Anson 公司购置或支持的计算机、服务器或者网络。制定本条例的目的是为了保证全体员工和业务伙伴在使用 Anson 公司的计算设备进行工作时能够有效果、有效率、有道德、有纪律。

因特网使用声明

Anson 公司对用户在因特网上看到或下载到的内容不承担法律责任。因特网是一个全球范围的计算机网络,它包含数以百万计的信息。在此警告用户:其中的许多信息可能有挑衅、色情或不正当的内容。要想在使用因特网的时候完全回避这些内容是很困难的。在因特网上查找资料时可能会进入一些有高度侮辱性内容的站点。此外,拥有因特网电子邮件地址可能会收到包含挑衅内容的不正当的电子邮件。在此声明:访问因特网的用户必须自己承担随之而来的风险。

在下面的文字里,“用户”指的是 Anson 公司员工和使用 Anson 公司计算系统和设备的合同商。

用户不得尝试在没有授权的情况下访问 Anson 公司网络系统上的数据和程序,也不得在没有主人同意的情况下访问其私用数据和程序。

用户有责任保护自己账户中使用或存储的信息资料。

如果用户发现以下情况,必须立刻向安防执行官报告:计算机安防方面的漏洞、因使用不当造成的事故或者其他违反本条例的行为。

用户不得在没有授权的情况下安装拨号调制解调器或回拨调制解调器。用户不得与他人共享自立的计算机或网络账户口令字。用户不得在没有授权的情况下复制他人的版权材料,除非法律允许或得到版权拥有者的许可。版权材料包括但不限于软件、电子文档、视频文件和音频文件。用户不得复制系统配置文件(如/etc/passwd 或 SAM 文件)供个人非授权使用,也不得提供给其他人做非授权使用。用户不得故意从事下列活动:骚扰其他用户、降低系统运行性能、剥夺 Anson 公司授权用户对某项资源的访问、额外侵占不属于自己的资源、遏止 Anson 公司的计算机安防措施、在没有授权的情况下获取 Anson 公司网络中某个系统的访问权。

电子通信和存储设备包括但不限于电子邮件服务器、文件服务器等,仅供公司工作使用。欺诈、骚扰、调戏、色情、恐吓、诽谤或者其他非法或不正当消息和/或不正当材料不得在 Anson 公司的网络上收、发、存储。

用户不得在没有发信人书面许可的情况下把电子邮件转发给其他人或其他地方。此外,用户不得发起或转发传销性质的电子邮件。

通信内容必须言简意赅。用户必须以对待其他书面材料同样的认真态度来起草电子邮件和其他电子文档。用计算机编写的任何东西都可能也确实会被其他人看到。

用户不得下载、安装或运行暴露系统安防弱点的安防检查程序。例如,Anson 公司用户不得在 Anson 公司的计算机系统上运行口令字破解程序。

用户不得过度消耗网络带宽，例如下载MP3、Real Audio音频文件或收听、收看网络电台、电视台，除非这是他们工作责任的一部分。

违反本条例的行为由经理会检查核实。纪律处罚以及纪律处罚的终止由经理会根据其情节的轻重决定。

计算机资源使用条例的补充规定

Anson公司的某些岗位需要运行针对网络或系统的安防分析程序。为了能够在Anson公司完成这类工作，Anson公司中的下列人员有权下载和运行任何必要的程序。

安防执行官：xx

系统管理员：yy

网络分析员：zz

信息保护条例

以下是Anson公司员工在处理、保护、传输信息资料时必须遵守的规章制度。制定本条例的目的是为了保证敏感信息和无形资产都能得到适当的保护，不会被恶意修改或公开。

美国商业保密法（UTSA）对公司商业秘密作出了如下的定义："配方、图案、资料汇编、程序、设备、方法、技术或工艺等符合保密要求的信息，具备独特的商业利益——真实的或潜在的、不广为人知、其他人尚未有适当手段获取其诀窍，但公开后这些人将获取经济利益，并且为保守这个秘密所做的努力合理合法。"我们把无形资产定义为不属于公共范畴的一切信息。

在下面的文字里，"用户"指的是Anson公司员工和使用Anson公司计算系统与设备的合同商。"第三方"指的是其他公司或不是Anson公司员工的自然人。

在接受或讨论商业秘密或无形资产之前，第三方必须签署保密协议。公司的无形资产、商业秘密或保密资料严格禁止向外界发送、传输或者以其他方式被传播。根据1996年颁布的《经济间谍法》（*Economic Espionage Act*），未经授权而传播这类信息会导致民事诉讼，甚至严重的刑事惩罚。商业秘密和无形资产必须保存在专用的文件服务器上。保存在个人机器（笔记本电脑、桌面电脑等）里的商业秘密和无形资产必须加密。经由公共网络（如因特网）传输的商业秘密和无形资产必须加密并加上数字签名。有公司外部来源的文件可能带有修改或破坏Anson公司计算机中文件的病毒，因此，从外界接收到的一切文件必须用公司认可的杀毒软件进行处理。

用户账户管理条例

以下是在Anson公司的计算资源，包括放置在Anson公司的计算系统和Anson公司使用的计算系统上申请用户和保有用户账号所必须遵守的规章制度。

下面的文字里，"用户"指的是Anson公司员工和使用Anson公司计算机系统与设备的合同商。

开设新账户的申请必须由CEO批准。

开设在公司计算系统上的账户只能由Anson公司员工本人使用，特殊权限需要提请CEO批准。

每个用户都有他/她自己的账户；在未经CEO批准的情况下，用户之间不得共享账户。

如果账户超过30天没有被使用过，将由系统管理员禁用。如果用户离职或退休，其

账户将在他离开公司的那一天起被禁用。用户账户的口令字必须遵守以下规则：

- 口令字至少要有7个字符长，必须由字母和数字字符组合而成；
- 口令字每隔60天必须更换；
- 新口令不得与前6次使用的口令字相同。

远程访问管理条例

以下是远程访问Anson公司的技术资源时必须遵守的规章制度，这里所说的技术资源指的是放置在Anson公司的计算系统和Anson公司使用的计算系统；其中包括但不限于由Anson公司购置或支持的计算机、服务器或者网络。制订本条例的目的是为了保证全体员工和业务伙伴在使用Anson公司的计算设备进行工作时能够有效果、有安全保障。

下面的文字里，“用户”指的是Anson公司员工和使用Anson公司计算机系统与设备的合同商。

全体用户都有Anson公司计算系统的远程访问权。

用户可以通过Anson公司远程访问解决方案所支持的各种手段（例如拨号ISP账户、ISDN、有线电视调制解调器或xDSL等）来连接上Anson公司的网络系统。如果用户在连接Anson公司计算资源时使用的是某种“常开”形式的因特网连接手段（例如宽带调制解调器、xDSL等），就必须在他们家里的PC上安装病毒扫描软件并实现安防方面的解决方案。

6. 风险评估

(1) 介绍。

风险评估指对各种可能的安全问题进行的估计，以掌握、分析电子商务活动面临的安全程度。风险评估主要回答7个问题：

① 什么事件会发生？（威胁代理）

② 如果它发生，最坏的影响是什么？（单次损失值）

③ 它发生的频率是什么？

④ 前3个问题的答案有多确定？（不确定性）

⑤ 我们可以采取哪些措施消除、减轻或转移风险？（安防控制措施）

⑥ 它需要花费多少资金？（安防控制措施成本）

⑦ 有效性有多大？（成本/收益分析或投资回报分析）

(2) 步骤举例。

第一步：资产清单、定义和要求。

① 确定企业关键性的商务活动；

② 编制关键性商务活动使用的资产清单；

③ 对这些资产进行估价，也可以使用能区分它们重要性的其他方法。

第二步：脆弱性和威胁评估。

① 运行自动化安防工具软件开始分析工作；

② 人工复查。

第三步：安防控制措施评估。

认真考虑各种安防措施以及它们的实施成本。

第四步：分析、决策和文档。

① 各种威胁的安防控制措施及实施成本分析表；

② 针对威胁选定将要实施的安防控制措施，或者不采取任何措施；

③ 编写评估工作报告，得出结论。

第五步：沟通和交流。

与有关方面沟通评估结论。

第六步：监督实施。

密切注意和分析新的威胁并对安防控制措施做必要的修改。企业的重大变革将导致一次新的风险评估过程。

(3) 案例参考。

背景介绍：B2B公司Anson是一家矿山设备出租代理的电子商务公司，所有的商务活动在网络上完成：打算出租设备的公司在Anson的主页上登记相关事项(包括设备型号、目前处于何处、联系方法和可出租时间等)，并向Anson公司交纳设备价值5%的登记费；需要租用的公司在Anson的主页上查找相应的资料，完成租借。Anson公司可以作为租金支付的第三方，也可由租借双方通过各自的银行进行租金支付。

评估过程：

第一步：资产清单、定义和要求。

① 确定企业关键性的商务活动。问题：利润从哪里来？公司内部沟通的手段如何？关键数据保存在哪里？如何修改这些数据？源代码保存在哪里？如何修改？登记费收入使用电信线路或银行收取。关键数据是关于设备登记方的登记信息，保存在Oracle数据库中，登记方或公司数据库管理员有权修改。源代码放在公司子网上，由程序员通过"质量保证体系"修改。

关键的业务流程：付款、收款安排；更新Web站点；浏览Web站点；公司及公司与客户的沟通。

② 编制关键性商务活动使用的资产清单。

问题：应保证上述关键活动的设备。

硬件：服务器、路由器等。

软件：网络服务和协议(HTTP、SMTP等)；远程访问地点；网络上传递的信息；什么时间，哪些人可以访问哪些东西。

③ 对这些资产进行估价，也可以使用能区分它们重要性的其他方法。

问题：评估的价格大多以该设备失效造成的损失为准，如表3-13-1所示。

表3-13-1　资产估价

设备名称	估　价
Web服务器	$10 000
数据库	$100 000
邮件服务器	$10 000
邮件客户端软件	$5000

第二步：脆弱性和威胁评估，如表 3-13-2 和表 3-13-3 所示。

表 3-13-2 脆弱性评估

软件名称	出处	能扫描的脆弱点数量	备注
SAFESuite	ISS 公司	236 种	由 Internet Scanner 和 System Scanner 组成
Kane Security Analyst	Instrusiton. com 公司	不针对特定脆弱点	从 6 个关键安防领域对系统进行检查
WebTrends Security Analyzer	www. webtrends. com	Linux 和 Windows 脆弱点	生成 HTML 格式的报告
Cerberus Internet Scanner	www. cerberus-infosec. com	126 种	自由软件

表 3-13-3 攻击频率清单

威胁	概率
非授权用户修改了数据库	30%
非授权用户看到了数据库内容，特别是银行账户	30%
攻击者或恶意用户获得了 Web 服务器的控制权	50%
Web 服务器或电子邮件服务器遭受拒绝服务攻击	80%
电子邮件病毒	90%
攻击者或恶意用户修改了 Anson 公司邮件服务器的电子邮件地址 25%	
普通攻击	90%

第三步：安防控制措施评估，如表 3-13-4 所示。

表 3-13-4 安防控制措施评估

威胁	可用的控制措施	成本
非授权用户修改了数据库	加强访问权限控制	$ 25 000
非授权用户看到了数据库内容，特别是银行账户	数据加密	$ 5000
攻击者或恶意用户获得了 Web 服务器的控制权	防火墙	$ 10 000
	入侵检测	$ 10 000
	入侵抵抗	$ 10 000
	文件完整性	$ 8000
	安装操作系统升级或补丁	$ 10 000
	选用加强型操作系统和服务器	$ 20 000
Web 服务器或电子邮件服务器遭受拒绝服务攻击	边境保护（防火墙或路由器）	$ 10 000
电子邮件病毒	电子邮件杀毒软件	$ 5000
	客户程序杀毒软件	$ 10 000
	控制使用电子邮件的附件	$ 100

续表

威　　胁	可用的控制措施	成本
攻击者或恶意用户修改了 Anson 公司邮件服务器的电子邮件地址	正确配置邮件服务器	$ 10 000
	监控外围的 SMTP 连接	$ 50 000
普通攻击	防火墙	$ 10 000
	入侵检测	$ 10 000
	入侵抵抗	$ 10 000

第四步：分析、决策和文档。

把实施成本和资产价值进行比较，包括运营、维护、学习使用、升级扩展、运行等方面的内容，让更多的人参与进来，最后形成文档。

Anson 公司安防控制措施及实施成本决策表如表 3-13-5 所示。

表 3-13-5　Anson 公司安防控制措施及实施成本决策表

威　　胁	可用的控制措施	成本
非授权用户修改了数据库	加强访问权限控制	$ 25 000
非授权用户看到了数据库内容，特别是银行账户	数据加密	$ 5000
攻击者或恶意用户获得了 Web 服务器的控制权	文件完整性	$ 8000
	安装操作系统升级或补丁	$ 10 000
	选用加强型操作系统和服务器	$ 20 000
Web 服务器或电子邮件服务器遭受拒绝服务攻击	边境保护(防火墙或路由器)	$ 10 000
电子邮件病毒	电子邮件杀毒软件	$ 5000
	客户程序杀毒软件	$ 10 000
	控制使用电子邮件的附件	$ 100
攻击者或恶意用户修改了 Anson 公司邮件服务器的电子邮件地址	正确配置邮件服务器	$ 10 000
普通攻击	防火墙	$ 10 000
	入侵检测	$ 10 000
	入侵抵抗	$ 5000

第五步：沟通和交流。

与有关方面沟通评估结论。

第六步：监督实施。密切注意和分析新的威胁并对安防控制措施做必要的修改。企业的重大变革将导致一次新的风险评估过程。

3.13.8　实验思考

企业风险评估一般从哪些方面进行？

3.14 安全审计与追踪

3.14.1 实验类型

综合型,4学时,课外自选实验。

3.14.2 实验目的

审计是记录使用计算机网络系统进行所有活动的过程,它是提高安全性的重要手段。它不仅能够识别谁访问了系统,还能指出系统正被怎样使用,对于确定有无攻击情况和确定攻击源很重要。通过实验,使学生了解安全审计的基本内容,掌握安全审计与追踪的分析方法。

3.14.3 题目描述

使用 TopSec TA-W 安全审计系统进行网络安全审计。

3.14.4 实验要求

理解安全审计的任务,能够根据实际需求部署审计系统,能够配置并使用 TopSec TA-W 安全审计系统。

3.14.5 相关知识

网络系统的安全与否是一个相对的概念,没有绝对的安全。在网络安全整体解决方案日益流行的今天,安全审计系统是网络安全体系中的一个重要环节。

企业客户对网络系统中的安全设备和网络设备、应用系统和运行状况进行全面的监测、分析、评估是保障网络安全的重要手段。网络安全是动态的,对已经建立的系统,如果没有实时的、集中的、可视化审计,就不能有效、及时地评估系统究竟是不是安全的,并及时发现安全隐患。所以安全系统需要集中的审计系统。在安全解决方案中,跨厂商产品的简单集合往往会存在漏洞,从而使威胁乘虚而入,危及安全。当某种安全漏洞出现时,如果必须针对不同厂商的技术和产品先进行人工分析,然后综合分析,提出解决方案,将降低对攻击的反应速度,并潜在地增加成本。如果不能将在同一网络中多个不同或者相同厂商的产品实现技术上的互操作,实现集中的审计,就无法发挥有效的安全性,无法有效管理。安全审计系统可以满足这些要求,对网络中的各种设备和系统进行集中的、可视的综合审计,及时发现安全隐患,提高安全系统成效。

1. 网络安全审计系统需要考虑的问题

(1) 日志格式兼容问题。一般情况下,不同厂商的设备或系统所产生的日志格式互不兼容,这为网络安全事件的集中分析带来了巨大难度。

(2) 日志数据的管理问题。日志数据量非常大,不断地增长,当超出限制后,不能简单地丢弃,需要一套完整的备份、恢复和处理机制。

(3) 日志数据的集中分析问题。一个攻击者可能同时对多个网络中的服务器发起攻击,如果单个地分析每个服务器上的日志信息,不但工作量大,而且很难发现攻击;如何将多个服务器上的日志关联起来,从而发现攻击的行为,是安全审计系统面临的重要问题。

(4) 分析报告及统计报表的自动生成机制。网络中每天会产生大量的日志信息,巨大的工作量使得管理员手工查看并分析各种日志内容是不现实的,必须提供一种直观的分析报告及统计报表的自动生成机制来保证管理员能够及时、有效地发现网络中各种异常状况及安全事件。

2. 网络安全审计系统的主要功能

(1) 采集多种类型的日志数据。能采集各种操作系统的日志、防火墙系统日志、入侵检测系统日志、网络交换及路由设备的日志和各种服务及应用系统日志。

(2) 日志管理。多种日志格式的统一管理。自动将其收集到的各种日志格式转换为统一的日志格式,便于对各种复杂日志信息的统一管理与处理。

(3) 日志查询。支持以多种方式查询网络中的日志记录信息,以报表的形式显示。

(4) 入侵检测。使用多种内置的相关性规则,对分布在网络中的设备产生的日志及报警信息进行相关性分析,从而检测出单个系统难以发现的安全事件。

(5) 自动生成安全分析报告。根据日志数据库记录的日志数据,分析网络或系统的安全性,并输出安全性分析报告。报告的输出可以根据预先定义的条件自动地产生、提交给管理员。

(6) 网络状态实时监视。可以监视运行有代理的特定设备的状态、网络设备、日志内容、网络行为等情况。

(7) 事件响应机制。当审计系统检测到安全事件的时候,可以采用相关的响应方式报警。

(8) 集中管理。审计系统通过提供一个统一的集中管理平台,实现对日志代理、安全审计中心、日志数据库的集中管理。

网络安全审计系统作为一个独立的软件,和其他的安全产品(如防火墙、入侵检测系统、漏洞扫描系统等)在功能上互相独立,但是同时又能互相协调、补充,保护网络的整体安全。本实验使用的设备和配套软件系统为 TopSec TA-W,详细内容可参考《网络卫士安全审计系统 TA-W 安装手册》、《网络卫士安全审计系统 TA-W 用户手册》等。

3.14.6 实验设备

主流配置 PC 一台,Windows 操作系统,TopSec TA-W 安全审计引擎与配套软件,网络环境。

3.14.7 实验步骤

1. TopSec TA-W 安全审计系统的部署

TopSec TA-W 安全审计系统的部署如图 3-14-1 所示。

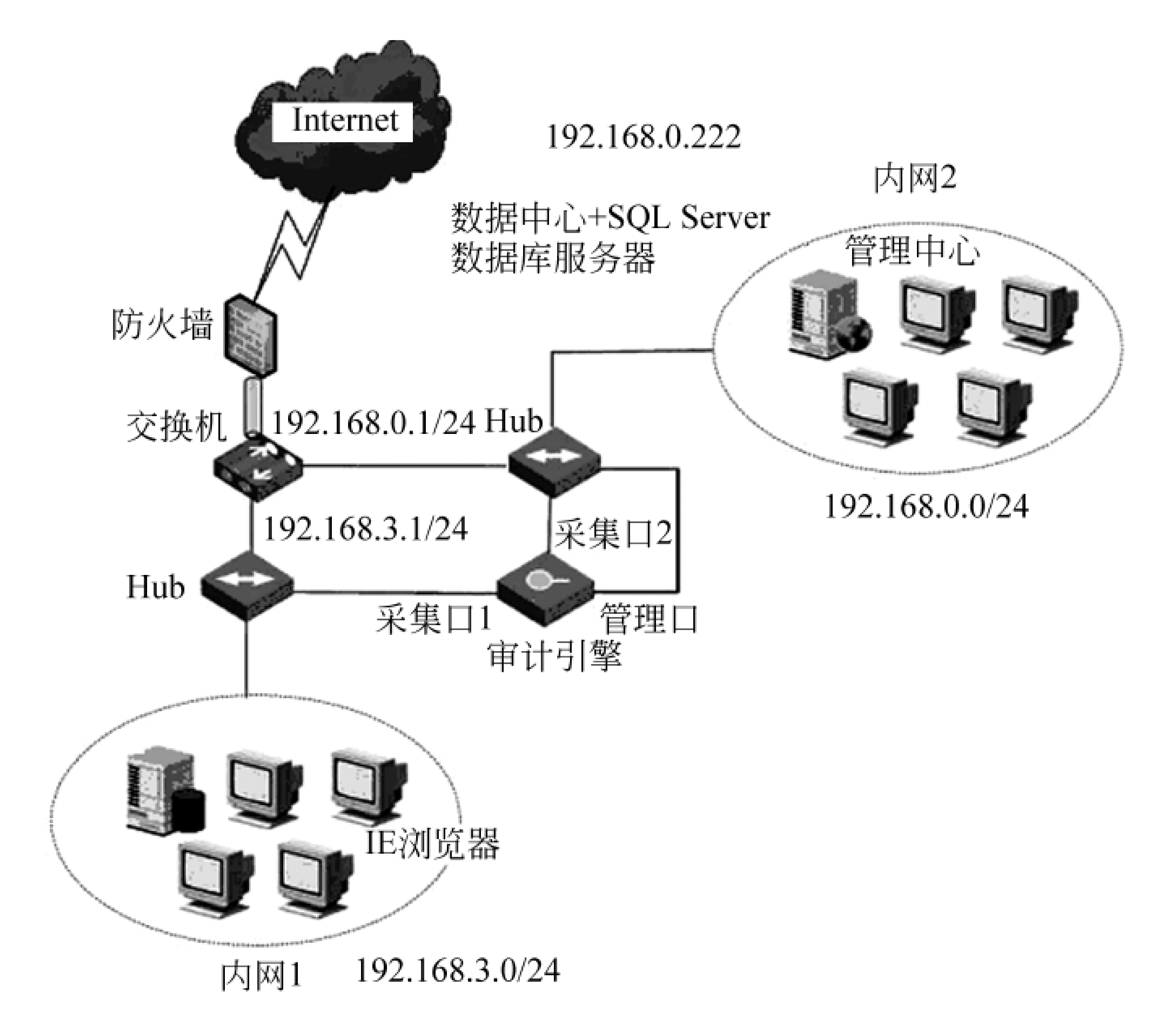


图 3-14-1 审计系统的部署

2. 初步配置

将一台本地管理主机通过 CONSOLE 线缆与审计引擎的 CONSOLE 口连接，初步配置审计引擎(一般情况下可以)。

3. 配置审计引擎

将管理口的 IP 地址设置为内网 2 的 IP 地址，为 192.168.0.254/255.255.255.0，网关地址为 192.168.0.1/255.255.255.0。步骤如下：

(1) TopsecTA-W#network reset //说明：管理口只允许有一个 IP 地址，因此首先必须将接口配置初始化

(2) TopsecTA-W#network interface eth0 ip add 192.168.0.254 mask 255.255.255.0

//说明：设置 eth0 口的 IP 地址和子网掩码

(3) TopsecTAW#network route add dst 0.0.0.0 src 0.0.0.0 gw 192.168.0.1

//说明：保证当审计引擎和数据中心不在同一个网段时，它们之间能够正常通信

(4) TopsecTA-W#ta comm modify dc_ip 192.168.0.222 key TOPSEC_2005 encrypt high

//说明：设置数据中心地址、数据中心和审计引擎之间进行通信的共享密钥、数据传输的加密方法。"dc_ip=192.168.0.222 key TOPSEC_2005 encrypt high"为高加密传输

```
(5) TopsecTA-W#save                    //保存所作的修改
(6) TopsecTA-W#ta restart              //重新启动审计引擎,才能使修改生效。不是重启整个系统
```

4. 配置采集口

TA-W-S 支持一个采集口,即同时只能有一个接口可以采集数据。系统默认的管理口为 eth0,采集口为 eth1。如果想将采集口更改为 eth3,必须将 eth1 和 eth2 接口关闭掉,同时开启 eth3 口,系统才会将 eth3 口作为采集口。步骤如下:

```
(1) TopsecTA-W#network interface eth1 shutdown       //关闭网口 eth1
(2) TopsecTA-W#network interface eth2 shutdown       //关闭网口 eth2
(3) TopsecTA-W#network interface eth3 no shutdown    //开启网口 eth3
(4) TopsecTA-W#save                                  //保存所作的修改
(5) TopsecTA-W#ta restart                            //重新启动审计引擎进程
```

5. 在服务器上安装数据中心(服务器的 IP 地址为 192.168.0.222)

数据中心负责存储来自审计引擎的各种信息,将数据存储在磁盘上,记录存储在 SQL Server 数据库中。一个数据中心可以存储管理多个审计引擎的数据。同时数据中心响应来自管理中心的查询请求,对原始数据报文进行还原和分析、统计分析,并将结果反馈给管理中心。另外,数据中心还负责转发来自管理中心的数据采集策略、报警响应策略以及流量监控策略到审计引擎。

数据中心的安装包括软件安装、配置 SQL Server 数据库、配置数据本地存储属性和配置连接密钥等,如图 3-14-2 所示。

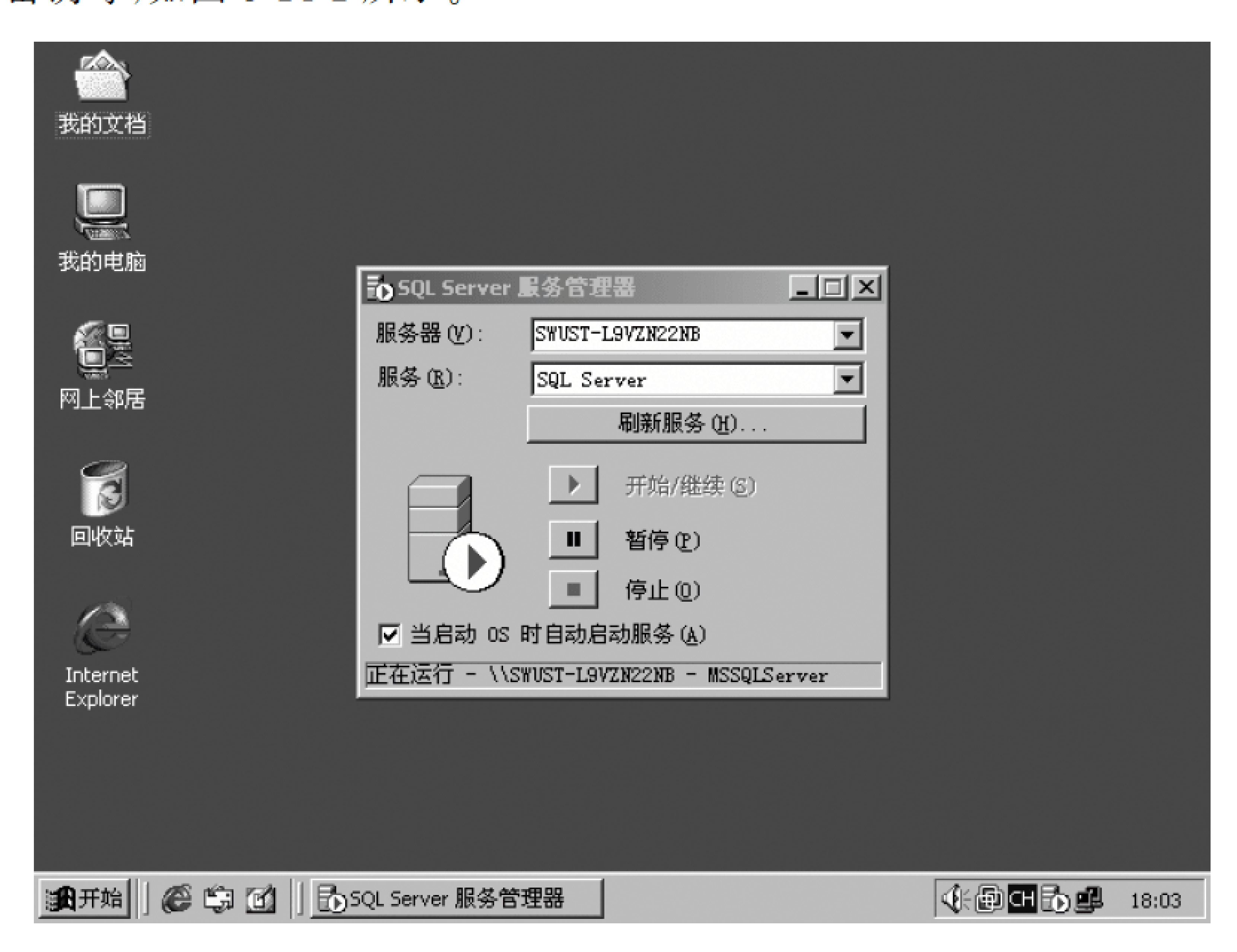


图 3-14-2 SQL Server 服务器运行状态

(1) 首先安装 SQL Server 2000。注意将“身份验证模式”设置为混合模式,用户名为 sa,密码为 xkd。

(2) 安装数据中心。在配置数据库的位置时选择“使用本地 SQL Server”,本地 SQL Server 服务器的名称为(local),SQL Server 的用户名为 sa,密码为 xkd。

配置数据中心其他属性设置:采集数据存放分区为 D:\(当然也可以放在其他分区,但不能是系统分区或者数据库系统分区,并且必须是 ntfs 格式),中心与管理中心预共享密钥为 TOPSEC_2005,引擎 IP 为 192.168.0.254,共享密钥为 TOPSEC_2005,如图 3-14-3所示。



图 3-14-3 数据中心属性设置

6. 在服务器上安装管理中心(服务器的 IP 地址为 192.168.0.222)

管理中心可以和一个或多个数据中心进行通信。用户可以通过 WEBUI 界面对管理中心、数据中心和审计引擎进行管理。

HTTP 和 HTTPS 协议的默认端口号为 80 和 443,如果这两个端口被其他服务占用,则必须在安装时修改默认端口号,否则安装包将提示用户重新输入端口号。

完成管理中心安装后,会自动启动 Apache 服务。Apache 服务启动成功后可以在“开始”菜单中选择“设置”→控制面板→“管理工具”→“服务”,查看到已经启动了 Apache 服务,如图 3-14-4 所示。

7. 配置数据中心

(1) 登录管理中心。管理员可以通过管理中心以 Web 访问的方式对管理中心进行远程管理。在访问时,管理员需要在管理主机的浏览器上输入管理中心的管理 URL,如图 3-14-5所示。如果修改了默认端口,须在 URL 后加上端口号。



图 3-14-4 查看 Apache 服务的启动状态

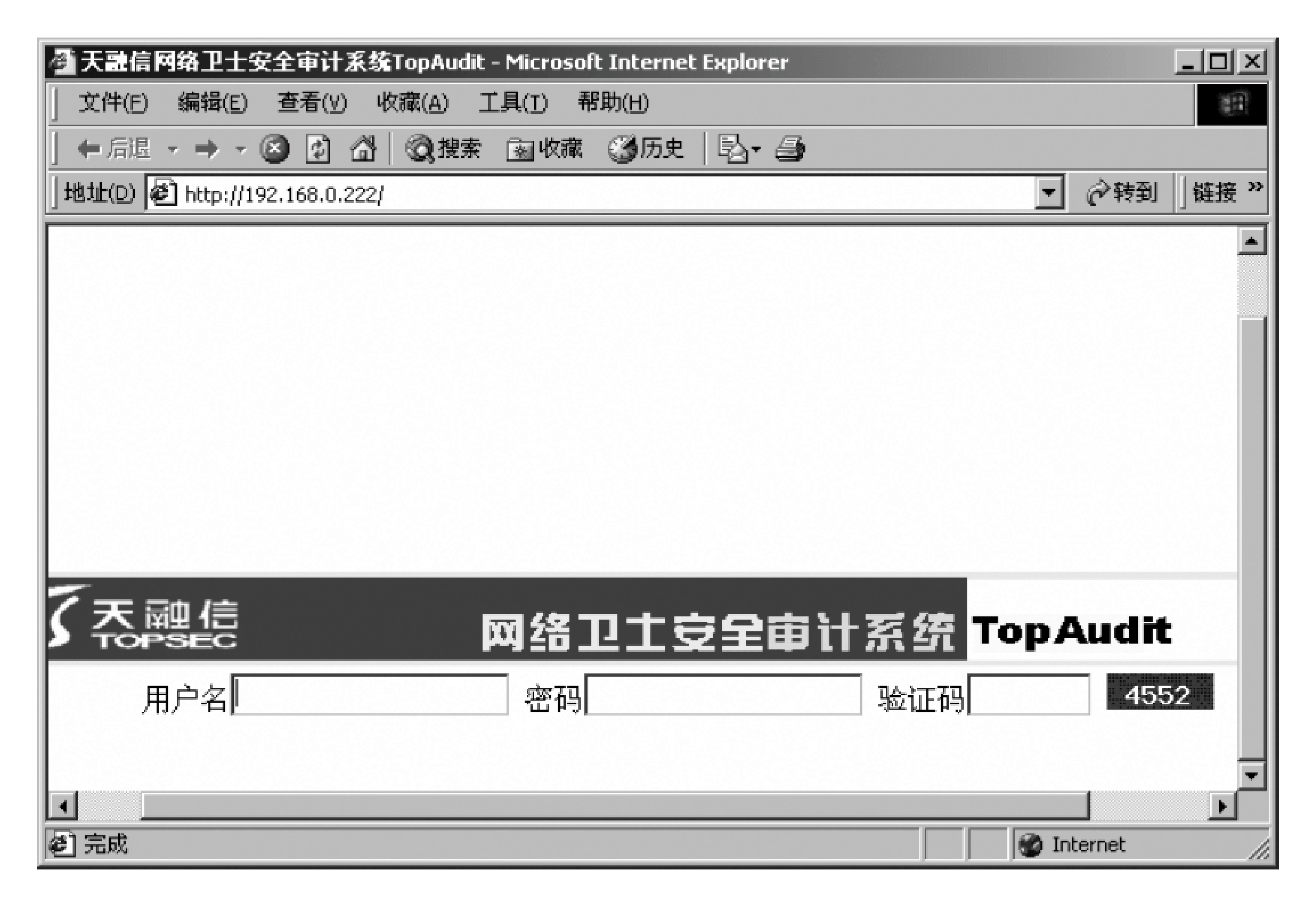


图 3-14-5 通过 URL 登录管理中心

输入用户名、密码后(管理中心的默认出厂用户名为 superman,密码为 talent),按照提示输入验证码,单击“登录”按钮就可以进入管理页面。

(2) 添加第一个数据中心。首次登录管理中心会直接进入添加数据中心界面,如图 3-14-6所示。

逐项填入数据中心的名称为“信息安全实验室数据中心”、所在主机 IP 地址为 192.168.0.222 及数据中心与管理中心通信的共享密钥,默认的共享密钥是“TOPSEC_2005”(大小写敏感)。单击“确定”按钮完成第一个数据中心添加,添加成功将有对话框提示。单击“确定”按钮,系统直接显示系统资源,包括刚刚添加的数据中心和从数据中心上传的审计引擎信息,如图 3-14-7 所示。

如果管理中心和多个数据中心进行通信,则还需要继续添加另外的数据中心。

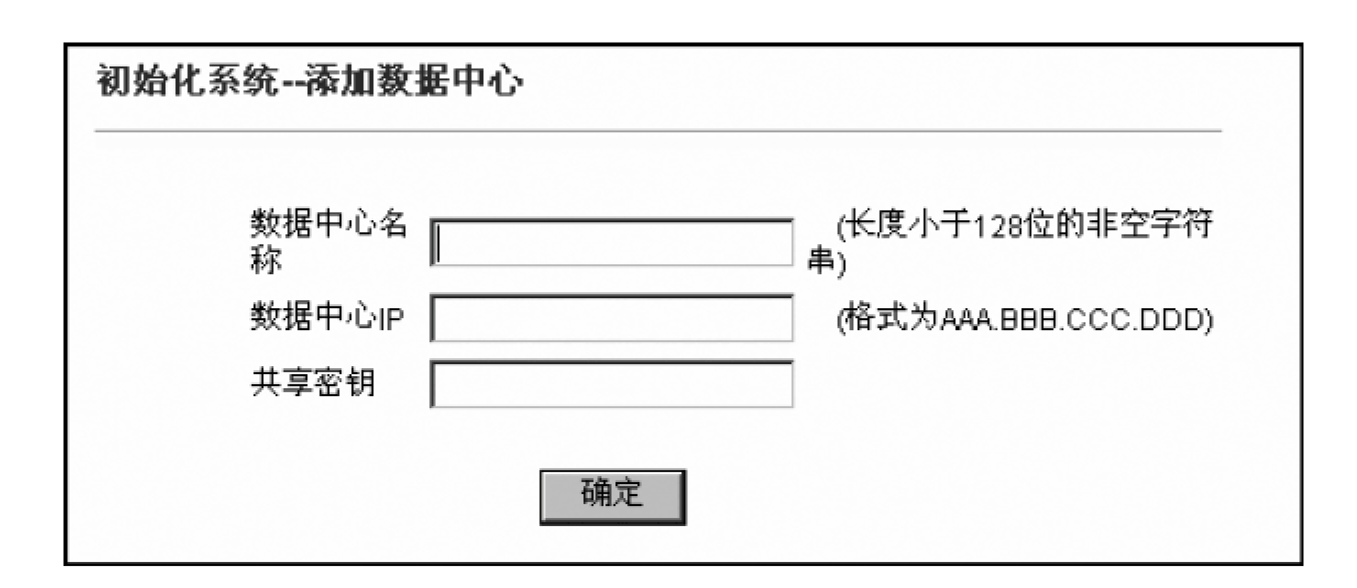
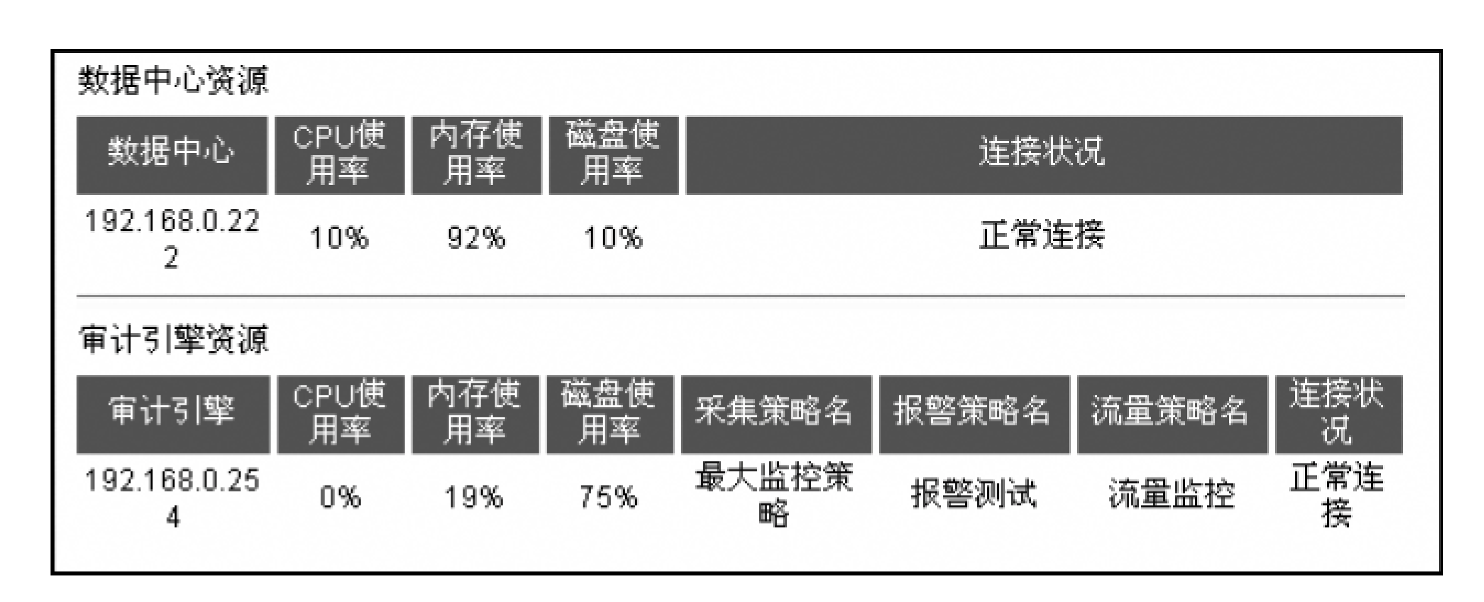


图 3-14-6　添加数据中心



数据中心资源

数据中心	CPU使用率	内存使用率	磁盘使用率	连接状况
192.168.0.222	10%	92%	10%	正常连接

审计引擎资源

审计引擎	CPU使用率	内存使用率	磁盘使用率	采集策略名	报警策略名	流量策略名	连接状况
192.168.0.254	0%	19%	75%	最大监控策略	报警测试	流量监控	正常连接

图 3-14-7　系统资源

8. 审计策略配置

超级管理员可以在管理中心为系统配置数据采集策略、报警响应策略和流量监控策略，并将已定义的策略通过数据中心下发到指定的审计引擎，审计引擎采集数据并根据采集策略对数据包进行过滤，还可根据报警响应策略做出实时的报警响应，同时发送报警日志到数据中心。

(1) 选择“审计策略”→“采集策略”→“策略分发”，单击“查看”按钮，就可以看到已经下发的默认监控策略，如图 3-14-8 所示。

策略名：　最大监控策略

协议	内容	端口	时间	IP段
HTTP	监控	80	00:00:00-23:59:59	0.0.0.0:255.255.255.255
FTP	监控	21	00:00:00-23:59:59	0.0.0.0:255.255.255.255
SMTP	监控	25	00:00:00-23:59:59	0.0.0.0:255.255.255.255
POP3	监控	110	00:00:00-23:59:59	0.0.0.0:255.255.255.255
TELNET	监控	23	00:00:00-23:59:59	0.0.0.0:255.255.255.255
MSN	监控	1863;80	00:00:00-23:59:59	0.0.0.0:255.255.255.255
WEBMAIL	监控	80	00:00:00-23:59:59	0.0.0.0:255.255.255.255
QQ	监控	80;443;8000	00:00:00-23:59:59	0.0.0.0:255.255.255.255
MMS	监控	1755	00:00:00-23:59:59	0.0.0.0:255.255.255.255
RTSP	监控	554	00:00:00-23:59:59	0.0.0.0:255.255.255.255

图 3-14-8　已经分发的监控策略

(2) 选择“审计策略”→“采集策略”→“策略分发”，单击“下发策略”按钮，选择审计引擎为“192.168.0.254”和下发策略名“最大还原策略”，单击“确定”按钮，就可以将指定的

策略下发到审计引擎，如图 3-14-9 所示。

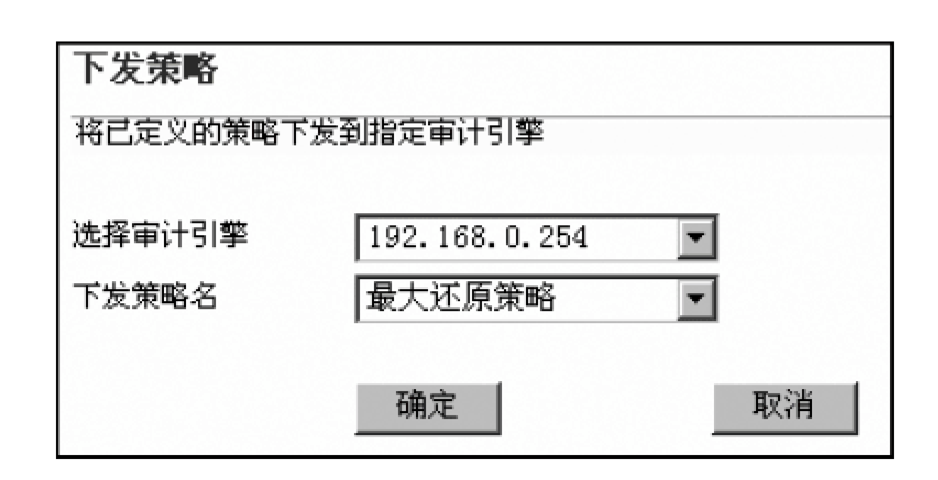


图 3-14-9　下发策略到审计引擎 192.168.0.254

（3）选择“审计策略”→“关键字策略”→“关键字管理”，单击“添加关键字”按钮，在出现的“添加关键字”页面进行设置，对出现的关键字进行审计。添加完成后单击“确定”按钮完成关键字的添加，如图 3-14-10 所示。

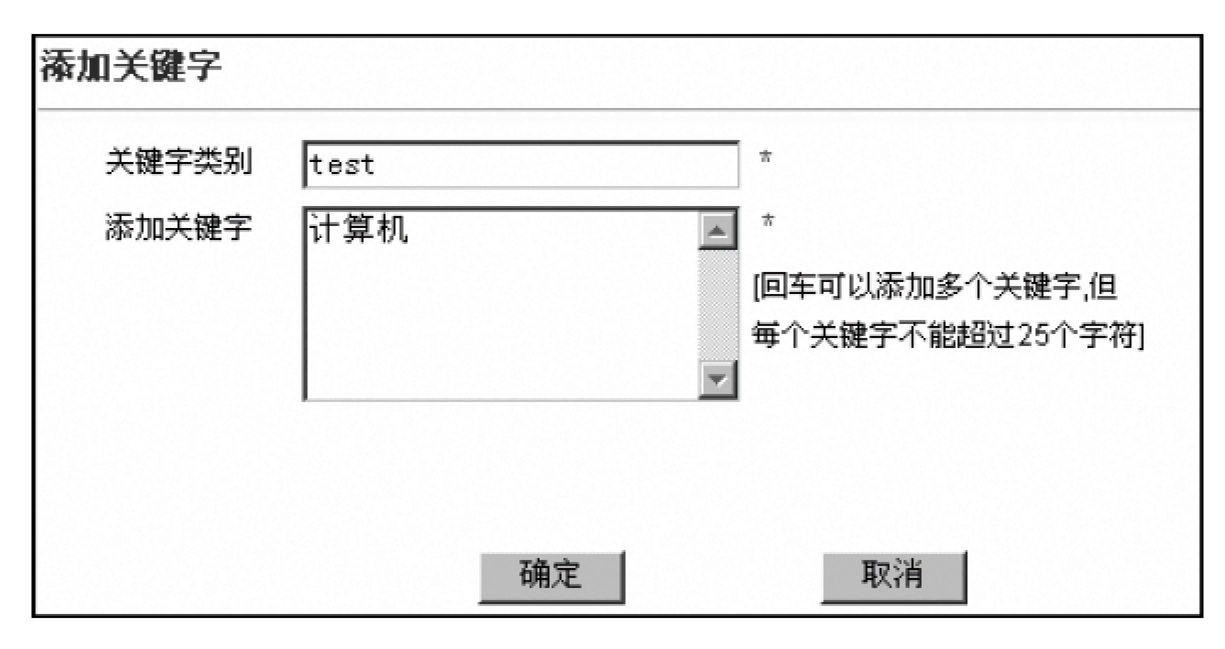


图 3-14-10　设置关键字审计

（4）选择“审计策略”→“关键字策略”→“关键字分发”，单击“下发关键字”按钮，在新开页面选择数据中心和关键字，单击“确定”按钮，完成下发，如图 3-14-11 所示。

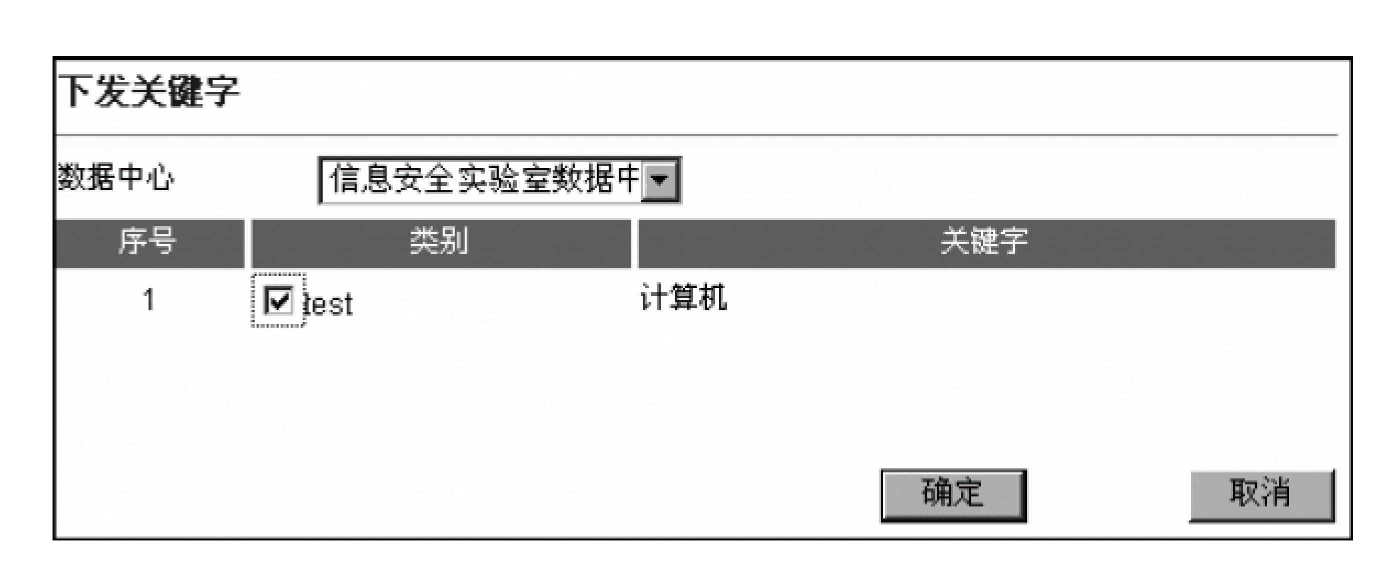


图 3-14-11　选择关键字和数据中心并下发关键字

（5）选择“审计策略”→“报警响应策略”→“报警策略”，单击“添加报警策略”按钮，在新开页面添加内容，对访问指定服务器的端口访问进行报警，如图 3-14-12 所示。单击“确定”按钮，完成添加。

（6）选择“审计策略”→“报警响应策略”→“策略分发”，单击“下发策略”按钮，在新开页面选择目的引擎和策略名，单击“确定”按钮，完成策略分发，如图 3-14-13 所示。

（7）选择“审计策略”→“流量监控策略”→“策略管理”，单击“添加策略”按钮，在新开页面进行填写，并单击“确定”按钮完成该策略的添加，如图 3-14-14 所示。

添加报警策略
策略名 访问80端口报警 *
报警协议 TCP
源IP
已定义IP any
自定义IP
起始IP * 结束IP *
目的IP
目的IP 222.196.35.2 * 目的端口 80 *
响应方式
响应方式 阻断 联动 邮件
确定 取消

图 3-14-12　报警策略设置

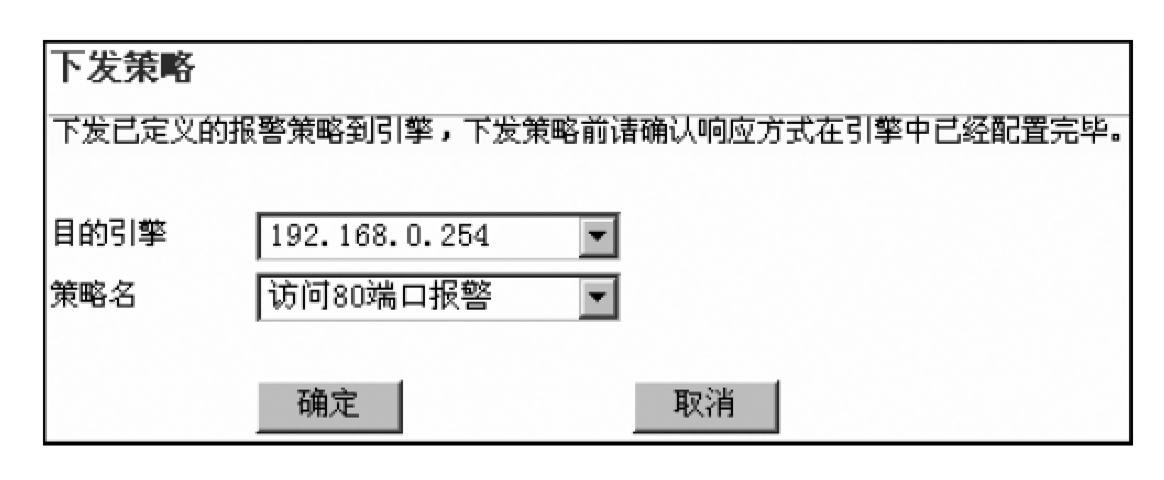


图 3-14-13　下发策略

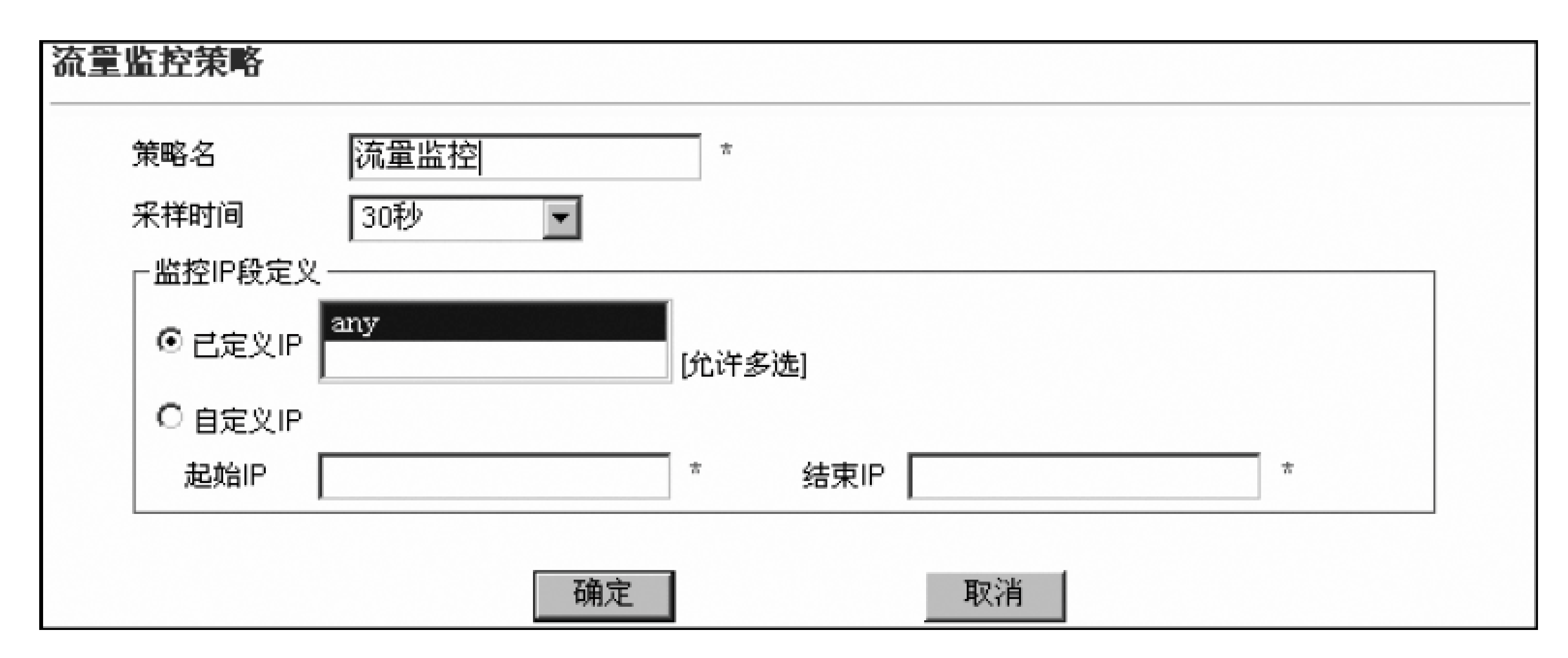


图 3-14-14　添加对整个网络的流量监控策略

(8) 选择“审计策略”→“流量监控策略”→“策略分发”，单击“下发策略”按钮，在新开页面选择引擎和策略名称，单击“确定”按钮，完成策略下发，如图 3-14-15 所示。

(9) 选择“系统管理”→“其他设置”→“引擎配置保存”页面，单击“确定”按钮，将审计策略保存到审计引擎，如图 3-14-16 所示。

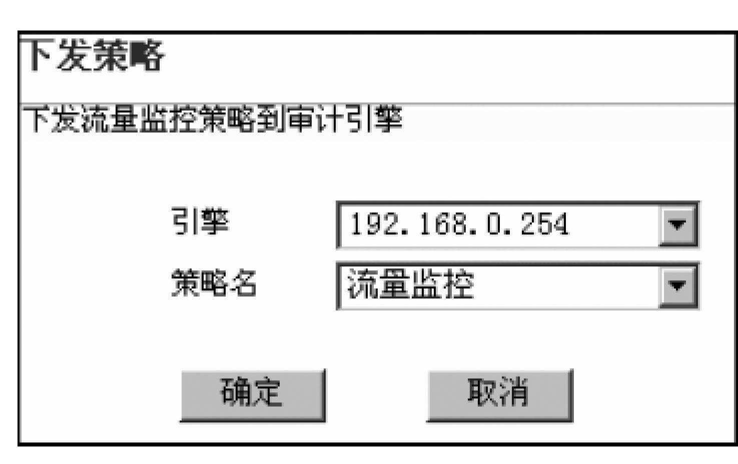


图 3-14-15　下发策略

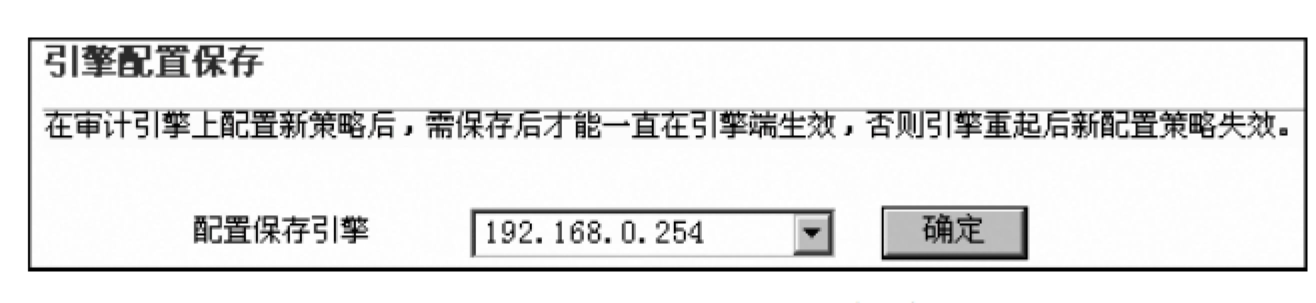


图 3-14-16　引擎配置保存

(10) 选择“实时监控”→“应用监控”，选择数据中心和应用协议，以及刷新频率和显示条数，单击“开始监控”按钮，就可以监控到相应应用协议的情况，如图 3-14-17 和图 3-14-18所示。



图 3-14-17　应用监控设置

序号	协议	时间	源IP	源端口	目的IP	目的端口	摘要
1	HTTP	2007-09-20 17:42:34	192.168.0.221	2949	202.115.160.9	80	get;http://news.swust.edu.cn/userfiles/l
2	HTTP	2007-09-20 17:42:34	192.168.0.221	2948	202.115.160.9	80	get;http://news.swust.edu.cn/newiii.asp
3	HTTP	2007-09-20 17:42:34	192.168.0.221	2947	202.115.160.9	80	get;http://news.swust.edu.cn/photo.asp
4	HTTP	2007-09-20 17:42:34	192.168.0.221	2946	202.115.160.7	80	get;http://www.swust.edu.cn/images/index
5	HTTP	2007-09-20 17:42:34	192.168.0.221	2945	202.115.160.7	80	get;http://www.swust.edu.cn/images/index
6	HTTP	2007-09-20 17:42:34	192.168.0.221	2944	202.115.160.7	80	get;http://www.swust.edu.cn/images/1.gif
7	HTTP	2007-09-20 17:42:34	192.168.0.221	2943	202.115.160.7	80	get;http://www.swust.edu.cn/images/index
8	HTTP	2007-09-20 17:42:34	192.168.0.221	2942	202.115.160.7	80	get;http://www.swust.edu.cn/images/space
9	HTTP	2007-09-20 17:42:34	192.168.0.221	2941	202.115.160.7	80	get;http://www.swust.edu.cn/images/index
10	HTTP	2007-09-20 17:42:34	192.168.0.221	2940	202.115.160.7	80	get;http://www.swust.edu.cn/images/index
11	HTTP	2007-09-20 17:42:34	192.168.0.221	2939	202.115.160.7	80	get;http://www.swust.edu.cn/css/sssccc.C
12	HTTP	2007-09-20 17:42:33	192.168.0.221	2938	202.115.160.7	80	get;http://www.swust.edu.cn/

图 3-14-18　HTTP 应用协议监控情况

(11) 选择“实时监控”→“流量监控设置”，在新开页面进行设置，单击“开始监控”按钮，就可以监控到各个 IP 地址主机的流量信息，如图 3-14-19 所示。



图 3-14-19　流量监控设置

(12) 选择“实时监控”→“报警监控”，单击“开始监控”按钮，然后打开浏览器，访问 222.196.35.2，就可以看到相应的报警信息，如图 3-14-20 所示。

报警响应记录　　更改监控条件　　停止

序号	时间	审计引擎	优先级	源地址	源端口	目的地址	目的端口	响应方式
1	2007-09-20 18:14:18	192.168.0.254	1	192.168.0.221	3130	222.196.35.2	80	不响应
2	2007-09-20 18:14:18	192.168.0.254	1	192.168.0.221	3131	222.196.35.2	80	不响应
3	2007-09-20 18:14:18	192.168.0.254	1	192.168.0.221	3129	222.196.35.2	80	不响应
4	2007-09-20 18:14:18	192.168.0.254	1	192.168.0.221	3128	222.196.35.2	80	不响应

图 3-14-20　报警响应记录

(13) 选择“安全审计”→“行为审计”→“行为审计”，选择开始时间、结束时间等，单击“审计”按钮，就可以查看相应的审计结果，如图 3-14-21 所示。

审计结果　　第一页　上一页　下一页

序号	时间	源IP	目的IP	源端口	目的端口	协议	内容摘要
1	2007-09-20 18:21:33	192.168.0.221	202.115.160.7	3292	80	HTTP	get;http://www.swust.edu.cn/
2	2007-09-20 18:21:33	192.168.0.221	202.115.160.9	3295	80	HTTP	get;http://news.swust.edu.cn/photo.asp
3	2007-09-20 18:21:33	192.168.0.221	202.115.160.9	3296	80	HTTP	get;http://news.swust.edu.cn/newiii.asp
4	2007-09-20 18:21:08	192.168.0.221	72.247.202.70	3282	80	HTTP	get;http://fpdownload.macromedia.com/pub/flash p...
5	2007-09-20 18:20:53	192.168.0.221	222.196.35.2	3303	80	HTTP	get;http://www.cs.swust.edu.cn/
6	2007-09-20 18:18:54	192.168.0.221	202.115.160.34	3270	80	HTTP	get;http://mail.swust.edu.cn/cgi-bin/listmail?f...
7	2007-09-20 18:18:53	192.168.0.221	202.115.160.34	3269	80	HTTP	post;http://mail.swust.edu.cn/cgi-bin/email
8	2007-09-20 18:18:48	192.168.0.221	202.115.160.14	3229	80	HTTP	get;http://202.115.160.14/userviewmail/usermail...
9	2007-09-20 18:18:48	192.168.0.221	202.115.160.14	3228	80	HTTP	get;http://202.115.160.14/userviewmail/useracti...

图 3-14-21　内容回放审计结果

(14) 选择“安全审计”→“内容审计”→“内容回放”，选择开始时间、结束时间等，单击“审计”按钮，就可以查看相应的审计结果。单击相应的“内容摘要”，可以看到相关内容，如图 3-14-22 所示。



图 3-14-22　显示内容回放的详细信息

(15) 选择“安全审计”→“内容审计”→“关键字审计”，选择相应的内容，单击“审计”按钮，就可以看到相应的内容审计结果。单击“内容摘要”，可以看到相应的内容，如图 3-14-23所示。

审计结果　　第一页　上一页　下一页

序号	时间	源IP	目的IP	源端口	目的端口	协议	内容摘要
1	2007-09-20 18:30:36	192.168.0.221	218.64.72.120	3349	80	HTTP	get;http://www.biaoshu.com/
2	2007-09-20 18:20:53	192.168.0.221	222.196.35.2	3303	80	HTTP	get;http://www.cs.swust.edu.cn/
3	2007-09-20 18:18:53	192.168.0.221	202.115.160.34	3269	80	HTTP	post;http://mail.swust.edu.cn/cgi-bin/email
4	2007-09-20 18:17:05	192.168.0.221	222.196.35.2	3158	80	HTTP	get;http://222.196.35.2/
5	2007-09-20 18:14:34	192.168.0.221	222.196.35.2	3128	80	HTTP	get;http://222.196.35.2/
6	2007-09-20 18:14:02	192.168.0.221	222.196.35.2	3117	80	HTTP	get;http://222.196.35.2/
7	2007-09-20 18:06:16	192.168.0.221	222.196.35.2	3071	80	HTTP	get;http://222.196.35.2/

图 3-14-23　关键字审计结果

3.14.8 实验思考

(1) 审计引擎能不能工作于交换式的网络环境下？如果能的话，需要什么条件？
(2) 你认为 TA-W 审计系统在功能上可以有哪些方面的改进？

3.15 应急响应与灾难恢复

3.15.1 实验类型

设计型，4 学时，课外自选实验。

3.15.2 实验目的

很多弱点可以在风险管理控制过程中通过技术、管理或操作的方法消除，但理论上不可能消除所有的风险。应急响应与灾难恢复是风险管理的补充，其目的是从风险中恢复过来。通过实验，使学生认识应急响应与灾难恢复的作用，了解应急响应与灾难恢复的步骤和内容。

3.15.3 题目描述

根据案例制订数据库系统容灾方案。

3.15.4 实验要求

理解应急响应与容灾备份的重要性，理解应急响应的处理步骤和容灾备份需求的衡量指标、各种容灾方法及其特点，能够制订系统容灾方案。

3.15.5 相关知识

进入 21 世纪，网络技术的高速发展使物理世界中涉及政治、军事、经济、文化、外交、安全关系和利益的全球化、多级化的复杂的世界格局已经全面映射到开放的互联网体系中，由此形成了一个社会、技术一体化的复杂巨系统。面对国际互联网大环境，我们深刻认识到，完全杜绝互联网安全事件是不可能的，重要的是加强应急响应。

1. 应急响应定义

应急响应(Emergency Response/Incident Response)通常是指安全人员在遇到突发事件后所采取的措施和行动。突发事件是指影响一个系统正常工作的情况，这里的系统

包括主机范畴内的问题,也包括网络范畴内的问题,这种“情况”包括常见的黑客入侵、信息窃取等,也包括拒绝服务攻击、网络流量异常等。

2. 应急响应的必要性

我们从以下几个方面讨论应急响应的必要性。

(1) 安全事件影响严重。公共互联网正在面临严峻的安全挑战。从2000年以来,严重的互联网安全事件层出不穷,在世界范围内造成了严重的损失。尤其是2003年,发生了多起波及全球的大规模安全事件,仅网络蠕虫就造成了全球范围的重大网络安全危害。在中国,“杀手蠕虫”使全部骨干网络受到严重影响,部分骨干网国际出入口基本瘫痪;“口令蠕虫”蔓延到大部分骨干网络中,累计超过4万余台计算机受感染;“冲击波及冲击波清除者蠕虫”使受感染的主机累计超过200万台。可以预见,这种大规模网络安全事件将会继续给人类带来更加严重的威胁。

(2) 安全漏洞普遍、攻击和恶意代码流行。一方面,计算机网络和系统变得越来越复杂,计算机软件(包括操作系统和应用软件)的安全缺陷往往与软件的规模和复杂性成正比;另一方面,互联网中有大量用来危害网络的工具,这使得网络攻击变得越来越容易。应急响应有助于降低这些漏洞一旦被攻破所带来的影响。

(3) 网络和系统管理复杂。从管理的层次上讲,每一个组织都应该通过风险分析制订出完备的安全政策,然后根据安全政策制订防御措施和检测措施。但目前很少有组织能够做到这一点,而且随着业务的发展和变化,安全政策的更新也可能不及时。应急响应在一定程度上弥补了维护和安全政策的不足,并且应急响应也可以及时发现这些不足,从而增强维护工作,完善安全政策。

3. 应急事件处理的一般阶段

应急事件处理的一般阶段包括准备、确认、封锁、根除、恢复、跟踪6个阶段。第1阶段“准备”,以预防为主;第2阶段“确认”,确定事件性质和处理人;第3阶段“封锁”,即时采取的行动;第4阶段“根除”,长期的补救措施;第5阶段“恢复”,由备份恢复系统;第6阶段“跟踪”,关注系统恢复以后的安全状况。

4. 国外应急响应组织发展状况

1988年在美国发生“莫里斯蠕虫事件”后,美国国防部高级计划研究署(DARPA)紧急在卡内基梅隆大学(CMU)软件工程研究所成立了世界上第一个计算机紧急事件响应组(CERT/CC),用于收集处理与计算机安全有关的信息。CERT/CC成立后,世界各地纷纷成立了应急响应组织,如美国空军的AFCERT、澳大利亚的AusCERT等。

为了各响应组之间的信息交换与协调,1990年成立了第一个应急响应与安全组论坛(Forum of Incident Response and Security Teams,FIRST),其宗旨是使各成员能就安全漏洞、技术、管理等方面进行交流与合作,以实现国际间的信息共享和技术共享,最终达到联合防范计算机网络上的攻击行为。

2003年亚太地区成立了APCERT(Asia-Pacific Computer Emergency Response

Team),APCERT 的任务主要是促进亚太地区的国际间合作,发展安全事件的评估标准,推动信息与技术的交换共享,进行合作研究等。

5. 国内应急响应组织及应急体系建设情况

在中国,1999 年在清华大学成立了中国教育和科研网应急响应组(CCERT),是中国大陆第一个计算机安全应急响应组。2000 年 10 月,信息产业部组建了“计算机网络应急处理协调中心”,2001 年 8 月,组建“国家计算机网络应急处理协调中心”,2003 年 7 月更名为“国家计算机网络应急技术处理协调中心”(National Computer network Emergency Response technical Team/Coordination Center of China,CNCERT/CC)。CNCERT/CC 的具体业务范围是,收集、核实、汇总和发布有关网络安全的权威性信息,为国家关键部门提供应急处理服务,协调和指导国内其他应急处理单位的工作,与国际上的应急处理组织进行合作和交流。

2002 年 8 月,CNCERT/CC 代表中国成为 FIRST 的正式会员,2003 年 3 月 CNCERT/CC 入选为 APCERT 指导委员会的成员单位。目前 CNCERT/CC 已经与国际应急响应组织建立了广泛的技术、交流和合作关系,并在国际交流中,在职责、组织结构和技术水平上不断进行完善。

6. 灾难备份需求的衡量指标

灾备方案应是风险和成本的相应平衡。

实施灾难备份项目的第一步应该从“分析评估以确定灾难备份需求目标”开始。

(1) RTO(Recovery Time Objective):是指灾难发生后,从 I/T 系统当机导致业务停顿之刻开始,到 IT 系统恢复至可以支持各部门运作、业务恢复运营之时,此两点之间的时间段。

一般而言,RTO 时间越短,即意味着要求在更短的时间内恢复至可使用状态。虽然从管理的角度而言,RTO 时间越短越好,但是这同时也意味着更多成本的投入,即可能需要购买更快的存储设备或高可用性软件。

对于不同行业的企业来说,其 RTO 目标一般是不相同的。即使是在同一行业,各企业因业务发展规模的不同,其 RTO 目标也会不尽相同。

(2) RPO(Recovery Point Objective):是指从系统和应用数据而言,要实现能够恢复至可以支持各部门业务运作,系统及生产数据应恢复到怎样的更新程度。这种更新程度可以是上一周的备份数据,也可以是上一次交易的实时数据。

7. 重要系统灾难备份主要的实现方法

在目前的技术条件下,重要系统灾难备份主要的实现方法主要有以下几种:

(1) 基于应用本身的容灾——应用直接指向两个同时运作的数据中心,在任意一个中心活动情况下继续工作。

(2) 基于文件/数据库日志的容灾——通过复制数据库日志和数据文件方式,从生产中心向海量存储系统进行数据容灾。

(3) 基于复制磁盘的容灾——通过复制磁盘 I/O 的方式,从生产中心向海量存储系统进行数据容灾,根据复制设备的不同,又可以分为基于主机、基于磁盘阵列、基于智能

SAN 虚拟存储设备。

8. 软件容灾方法

软件容灾指对灾难发生(即生产系统出乎预料地失效)时的实时、自动地响应,能在冗余设备上快速将应用系统重新启动而只损失极少的数据。软件容灾是建立在高可用的基础上的,即如同在本地的硬件或软件失败时的响应一样。

(1) 容灾设计的软件需求。容灾软件能自动预知错误,具体的操作往往需要广泛的专业知识。容灾软件应该能对容灾架构经常进行低成本的、非破坏性的测试。容灾软件应能充分利用现有 IT 架构。

(2) 容灾设计的业务需求。容灾软件必须作为 DR 计划的一部分,能自动执行必要的步骤。必须预先定义目标恢复时间(RTO)和目标恢复点(RPO)。

(3) 容灾设计的物理需求。远程建立能随时启动的、冗余的主机、存储及网络结构。选择远程灾备中心时,它与生产中心的距离要合理。

9. 软件在容灾中的责任

(1) 应用系统管理:启动,关闭,监控,故障切换。

(2) 故障通知:确定应用的停止及如何响应。

(3) 数据迁移:在灾备中心随时提供最新的有效数据,而无须从磁带上恢复。

(4) 子网故障切换:能够将客户端从生产中心重定向到灾备中心。

10. 主要的容灾技术

(1) 基于存储的解决方案(也可以称为运行在磁盘阵列上的方案)。

基于存储的解决方案主要包括以下内容。

- EMC:SRDF;
- IBM:PPRC,XRC;
- HDS:HXRC;
- HP:Continuous Access。

这种方案的主要优点在于:

- 这种数据复制方式和服务器平台无关。

这种方案的主要缺点在于:

- 不同节点间必须采用同一个厂家的磁盘阵列(一般是高端阵列)才可以完成数据的复制,因此,所复制的数据具有局限性;
- 带宽需求较高,带来长期的、巨大的附加费用;
- 代价高昂;
- 读取磁盘中的数据加以远程传递,因此容易造成缓存中的数据丢失。

(2) 基于主机的解决方案(也可以称为运行在服务器上的解决方案)。

基于主机的解决方案主要包括 Veritas VVR 产品。

这种方案的主要优点在于:

■ 这种数据复制方式和服务器平台以及存储厂家无关。

这种方案的主要缺点在于：

■ 数据复制对应用系统的影响较大；

■ 造价昂贵；

■ 带宽要求较高；

■ 实施难度较大；

■ 延迟较大；

■ 读取磁盘中的数据加以远程传递，因此容易造成缓存中的数据丢失。

(3) IN-Band 方式的解决方案。

IN-Band 方式的解决方案主要包括以下内容。

■ Datacore：AIM；

■ FalconStor：IPStor；

■ HP：CASA。

这种方案的主要优点在于：

■ 这种数据复制方式和服务器平台以及存储厂家无关。

这种方案的主要缺点在于：

■ 难于扩展；

■ 延迟增加；

■ 高带宽要求；

■ 读取磁盘中的数据加以远程传递，因此容易造成缓存中的数据丢失。

11. 实例简介

VERITAS 的数据复制管理软件 VERITAS Volume Replicator 赛门铁克推出 Veritas Storage Foundation 5.0 HA for Windows FalconStor 公司 IPStor 存储管理软件为存储架构的容灾系统。

TrueCopy 数据远程容灾解决方案是结合 HDS Freedom 智能存储系统的特点推出的数据远程容灾解决方案。TrueCopy 是基于磁盘存储系统运行的软件包，不依赖任何主机操作系统和其他第三方厂商软件，为用户提供了安全、开放、经济和实用的远程容灾解决方案。

基于智能 SAN 虚拟存储设备进行磁盘复制的一个成熟的方案就是 IBM 的 SAN 卷控制器(SAN Volume Controller，SVC)。

3.15.6 实验设备

主流配置 PC，Windows 操作系统，网络环境。

3.15.7 实验步骤

以下是某广电公司数字电视存储系统容灾备份方案。

××广电近期在原有双机系统的前提下，提出对数据库系统进行远端灾难恢复，以保证系统更加强劲地运行。××广电数据库应用系统采用两台宝德 PT2350R 服务器加一台宝德 GS4008 存储柜，两台数据库服务器采用 Windows 2000 Server＋Oracle 8i 的数据库软件，组成双机系统。目前的数据库平台通过双机系统，已具备较高的可靠性，为了保证系统的无忧运行，需要进一步对基于 Oracle 数据库的双机系统进行灾备。

1. 系统需求分析

××广电对数据系统灾备提出了高标准的要求，一是在不改变原有双机系统的前提下组建新的灾备系统；二是机房系统数据存储池同灾备系统的存储保证时时备份（网络带宽有要求）或按时间点进行备份；三是在生产端出现整体故障的情况下，启动灾备端应用及存储系统，在远端提供正常的数据库服务；四是整体设计思路要先进，能够适应未来的发展需要。

根据××广电目前系统环境及未来发展需求，最终系统选定宝德存储容灾与管理软件和宝德服务器共同部署××广电的整体灾备环境，建立起针对性极强的灾备系统解决方案。

2. 灾备方案

本案例在生产端两台数据库服务器宝德 PR2350 上安装磁盘数据快照抓取软件宝德 Disk Safe 及 Snapshot for Oracle agent，作为整个系统灾备数据的发起端；在灾备端使用一台宝德服务器 PT6215，安装 Oracle 数据库，提供与生产端数据库服务器同样的服务；在 GS9016i 上安装 BizCON iSCSI Server 及 Snapshot Module 两个软件；将灾备端一台服务器及一台 GS9016i 通过交换机连入同一局域网，据此架构起××广电的整个灾备系统。灾难未发生，生产端系统正常工作，灾备端进行常规备份。一旦灾难发生，生产端系统宕机，灾备端就立即提供服务。

系统拓扑图如图 3-15-1 所示。

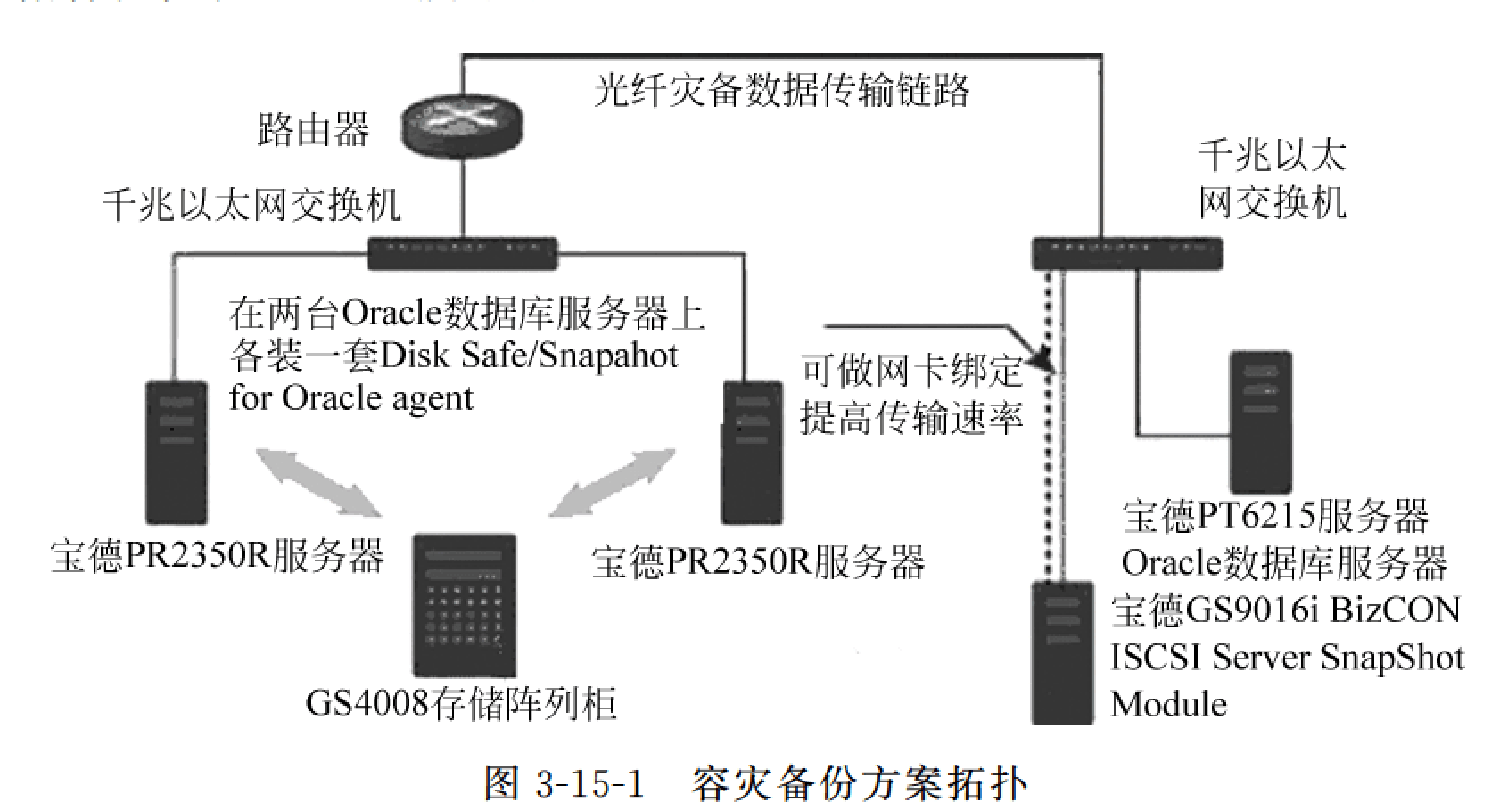


图 3-15-1 容灾备份方案拓扑

3. 灾备系统实施

灾备系统中，管理是关键。在××广电灾备系统存储管理的控制台中，宝德为其制订

了完备的灾备系统复制策略，管理员很方便地为将要复制的源盘定制相应的复制策略来控制复制进程，例如一天中的特定时间、持续时间间隔、容量的变化量、连续复制。这几种策略可以单独使用或组合使用，使得为管理员提供了一个非常灵活的策略触发机制，实现数据的保护而不受灾难的影响。

当在本地的磁盘卷被复制时，通过宝德灾备系统的控制台在远程站点为此卷建立相应的目标卷，并同时在本地的宝德灾备系统存储管理服务器及远程的存储管理服务器之间生成复制通道，每一次初始化的同步数据处理过程在正式执行定制复制之前进行。××广电灾备系统事先将数据复制到远端后，建立起两端的复制关系后只检查两端数据之间的差量，然后将差量数据从本地的宝德灾备系统存储管理服务器所管理的卷复制到远端存储管理服务器管理的卷中，待数据同步后，开始按照事先订制的策略触发复制进程。

宝德灾备系统的复制是基于磁盘卷进行操作的，按照上述策略触发复制进程，在本地应用服务器对于写的动作，只写到本地的磁盘卷中，当达到事先设定的触发条件时触发数据的复制，每次复制的数据都通过宝德灾备系统的 Snapshot Module 功能保护起来，因此数据在整个复制过程中不影响应用系统的正常业务处理。

同时，系统通过数据库代理模块对 Oracle 数据库提供 7×24 小时的在线数据保护，即不间断地为数据处理提供自动管理保护，结合宝德灾备系统安全可靠地进行数据的快照复制、零干扰备份、远程数据复制等高级存储服务功能。总体来看，本存储灾备系统实现了基于 Java 的异构存储设备集中管理，有效降低了硬件及维护管理的投资成本，实现了可靠的容灾系统及数据多重保护，为企业存储方案选型提供了良好的启示。

3.15.8 实验思考

(1) 应急响应的一般步骤是怎样的？

(2) 容灾方案的制订需考虑哪些因素？

参 考 文 献

[1] 史景慧.网络安全虚拟实验系统的设计与实现.北京邮电大学,2012-03-07.

[2] 郭艳来,崔益民,匡春光,等.网络安全试验平台研究.计算机工程与设计,2015-06-16.

[3] 戴士剑.数据恢复技术与方法探析.信息网络安全,2009-06-10.

[4] 杨智君,田地,马骏骁,等.入侵检测技术研究综述. 计算机工程与设计,2006-06-28.

[5] 王岫.基于 Snort 的入侵检测系统的研究与实现.北京交通大学,2010-06-01.

[6] 谭臻.校园网络安全管理中的黑客入侵与防范.计算机安全,2007-10-05.

[7] 薛玉芳.数据库安全及黑客入侵防范.安徽理工大学,2012-06-01.

[8] Lily Dong,Yuanzhen Peng. Network Security and Firewall Technology. Proceedings of 2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010 no. 2),2012-11-16.

[9] 罗新,王会林.网络实验室 VPN 实验项目的设计与实现.实验科学与技术,2012-06-28.

[10] 李长春.基于 IPSec 的 VPN 技术应用与研究.通化师范学院学报,2012-10-20.

[11] 詹峰.基于网络安全的一种新的漏洞检测系统方案.中国校外教育(理论),2007-09-15.

[12] Wei Lu. Network Intrusion Detection and Prevention [electronic resource]: Concepts and Techniques/Ali A. Ghorbani. New York:Springer,2010.

[13] 张惠林.PPP 协议分析及其在路由平台上的实现.天津大学,2007-01-01.

[14] 贺抒,梁昔明.NAT 技术分析及其在防火墙中的应用.微计算机信息,2005-01-10.

[15] 何蕾.面向应急响应的服务恢复机制研究与实现.国防科学技术大学,2008-11-01.

[16] 杨召军.基于 SNMP 协议的网络集中监控系统分析与设计.北京邮电大学,2011-06-01.

[17] 张卫东,王伟,韩维桓.网络流量测量与监控系统的设计与实现.计算机工程与应用,2005-3-2.

[18] 朱慧芳.基于 Web Service 的证书服务应用系统的研究与实现.上海交通大学,2008-01-01.

[19] 张成琦.高校机房服务器网络安全的分析与研究.湖南大学,2012-04-15.